

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-179609

(43)Date of publication of application : 27.06.2003

(51)Int.Cl.

H04L 12/28

G06F 15/00

H04L 9/32

H04Q 7/38

(21)Application number : 2002-202072

(71)Applicant : TAIKO DENKI CO LTD  
E WITH U:KK

(22)Date of filing : 11.07.2002

(72)Inventor : MAEDA MIKIO  
MATSUDA SHUNSUKE  
MIMURO SATORU

(30)Priority

Priority number : 2001243039

Priority date : 09.08.2001

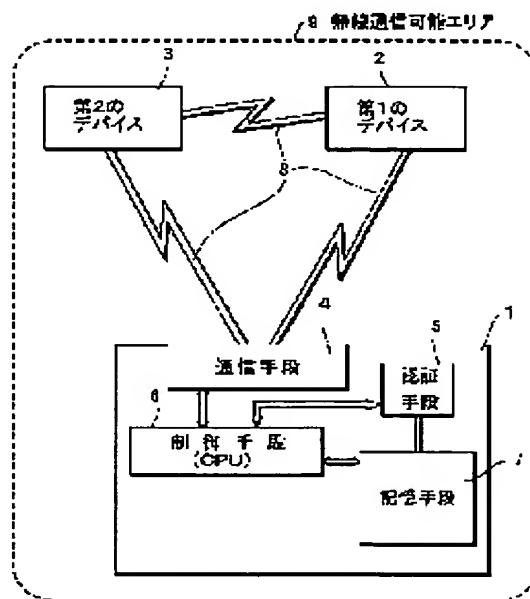
Priority country : JP

## (54) COMMUNICATION AUTHENTICATION DEVICE AND COMMUNICATION AUTHENTICATION METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a communication authentication device connected with variously constituted mobile terminals and house appliances of a Bluetooth (R) system by radio communication, for authenticating whether or not the connection of individual devices within the radio communication area is permitted before the mobile terminals and the house appliances of the Bluetooth (R) system start 'data communication'.

SOLUTION: The communication authentication device authenticates radio connection among the devices such as a portable terminal, a portable telephone, a personal computer and digital audio equipment, and is provided with a communication means performing the radio connection with the respective devices, an authentication means discriminating whether or not to enable transmission or reception of data between the devices, a control means controlling the communication means and the authentication means, and a storage means storing the data for authentication control used in the control means.



## LEGAL STATUS

[Date of request for examination] 12.07.2002

[Date of sending the examiner's decision of rejection] 24.05.2005

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection] 2005-11946

[Date of requesting appeal against examiner's decision of rejection] 23.06.2005

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2003-179609  
(P2003-179609A)

(43) 公開日 平成15年6月27日 (2003.6.27)

(51) IntCl. <sup>7</sup>	識別記号	F I	テーマコード <sup>*</sup> (参考)
H 0 4 L 12/28	3 0 0	H 0 4 L 12/28	3 0 0 Z 5 B 0 8 5
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 C 5 J 1 0 4
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 A 5 K 0 3 3
H 0 4 Q 7/38		H 0 4 B 7/26	1 0 9 R 5 K 0 6 7

審査請求 有 請求項の数17 O L (全 27 頁)

(21) 出願番号 特願2002-202072(P2002-202072)  
 (22) 出願日 平成14年7月11日 (2002.7.11)  
 (31) 優先権主張番号 特願2001-243039(P2001-243039)  
 (32) 優先日 平成13年8月9日 (2001.8.9)  
 (33) 優先権主張国 日本 (J P)

(71) 出願人 000205122  
大宏電機株式会社  
東京都大田区矢口3丁目7番3号  
 (71) 出願人 500529850  
株式会社イーウィズユー  
東京都品川区南大井6-17-17 FINE  
ビル  
 (72) 発明者 前田 幹夫  
東京都大田区矢口3丁目7番3号 大宏電  
機株式会社内  
 (74) 代理人 100087745  
弁理士 清水 善▲廣▼ (外2名)

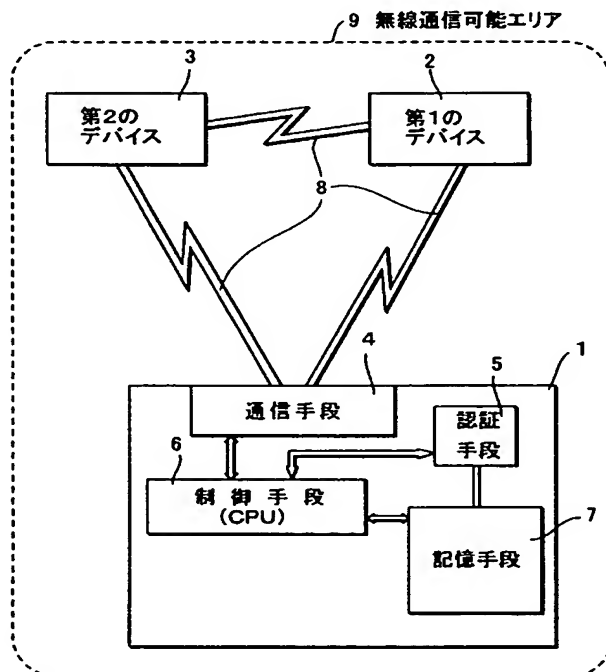
最終頁に続く

(54) 【発明の名称】 通信認証装置及び通信認証方法

(57) 【要約】

【課題】さまざまに構成されたブルートゥース方式のモバイル端末や家電装置と、無線通信で接続され、ブルートゥース方式のモバイル端末や家電装置が「データ通信」を開始する前に、個々の装置がその無線通信エリア内での接続許可されたものかどうか認証する通信認証装置を提供することを目的とする。

【解決手段】通信認証装置は、携帯端末、携帯電話、パーソナルコンピュータ、デジタル音響機器等のデバイス間の無線接続を認証する通信認証装置であって、それぞれの前記デバイスと無線接続を行う通信手段と、前記デバイス間のデータの送信又は受信を可能とするか否かを判別する認証手段と、前記通信手段と前記認証手段とを制御する制御手段と、前記制御手段で使用する認証制御用データを記憶する記憶手段とを有することを特徴とする。



## 【特許請求の範囲】

【請求項1】 携帯端末、携帯電話、パーソナルコンピュータ、デジタル音響機器等のデバイス間の無線接続を認証する通信認証装置であって、それぞれの前記デバイスと無線接続を行う通信手段と、前記デバイス間のデータの送信又は受信を可能とするか否かを判別する認証手段と、前記通信手段と前記認証手段とを制御する制御手段と、前記制御手段で使用する認証制御用データを記憶する記憶手段とを有することを特徴とする通信認証装置。

【請求項2】 前記記憶手段には、使用者の氏名、生年月日、電話番号、電子メールアドレス、免許証番号など複数の実際の個人データをパスワードとして記憶することを特徴とする請求項1に記載の通信認証装置。

【請求項3】 前記記憶手段の内部メモリに管理対象となるデバイスの情報を入力する入力手段と、前記ネットワークの通信状態や前記入力手段からの入力情報を表示する表示手段とを有することを特徴とする請求項1に記載の通信認証装置。

【請求項4】 前記制御手段に接続され、外部から起動ができる起動手段を備えたことを特徴とする請求項1に記載の通信認証装置。

【請求項5】 前記制御手段に接続され、あらかじめ決めた位置でのみ制御動作を行うための位置情報検出手段を備えたことを特徴とする請求項1に記載の通信認証装置。

【請求項6】 前記制御手段に接続され、使用者が設定した時刻や一定時間のみ制御手段からの通信命令や認証命令を動作させるタイマー手段を備えたことを特徴とする請求項1に記載の通信認証装置。

【請求項7】 通信認証装置と第1のデバイスと第2のデバイスとがそれぞれ無線通信で接続され、前記第1のデバイスと前記第2のデバイスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記第1のデバイスから前記第2のデバイスに対して接続要求を出す第1のステップと、第1のステップの後に、前記第2のデバイスが前記第1のデバイスへ接続してよいかどうかを、前記第2のデバイスから前記通信認証装置に対して問い合わせる第2のステップと、第2のステップの後に、前記通信認証装置が前記第1のデバイスの存在を確認する第3のステップと、第3のステップの後に、前記第1のデバイスから前記通信認証装置に対して前記第1のデバイスの存在情報を通知する第4のステップと、第4のステップの後に、前記通信認証装置が前記第1のデバイスの存在を確認した結果を、前記通信認証装置から前記第2のデバイスに対して報告する第5のステップと、第5のステップの後に、前記第1のデバイスと前記第2のデバイスの通信を開始する第6のステップとからなる通信認証方法。

【請求項8】 通信認証装置と第1のデバイスと第2のデバイスとがそれぞれ無線通信で接続され、前記第1の

デバイスと前記第2のデバイスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記第1のデバイスから前記第2のデバイスに対して接続要求を出す第1のステップと、第1のステップの後に、前記第2のデバイスが前記第1のデバイスへ接続してよいかどうかを、前記第2のデバイスから前記通信認証装置に対して問い合わせる第2のステップと、第2のステップの後に、前記通信認証装置と前記第1のデバイスの間で、前記第1のデバイスのアドレス情報又はパスワード情報を送受信することによって前記第1のデバイスを認証する第3のステップと、第3のステップの後に、前記通信認証装置から前記第2のデバイスに対して前記第1のデバイスが通信許可された装置であることを報告する第4のステップと、第4のステップの後に、前記第1のデバイスと前記第2のデバイスの通信を開始する第5のステップとからなる通信認証方法。

【請求項9】 通信認証装置と第1のデバイスと第2のデバイスとがそれぞれ無線通信で接続され、前記第1のデバイスと前記第2のデバイスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記第1のデバイスから前記第2のデバイスに対して接続要求を出す第1のステップと、第1のステップの後に、前記第2のデバイスが前記第1のデバイスへ接続してよいかどうかを、前記第2のデバイスから前記通信認証装置に対して問い合わせる第2のステップと、第2のステップの後に、前記通信認証装置と前記第2のデバイスの間で、前記第2のデバイスのアドレス情報又はパスワード情報を送受信することによって前記第2のデバイスを認証する第3のステップと、第3のステップの後に、前記通信認証装置と前記第1のデバイスの間で、前記第1のデバイスのアドレス情報又はパスワード情報を送受信することによって前記第1のデバイスを認証する第4のステップと、第4のステップの後に、前記通信認証装置から前記第2のデバイスに対して、前記第1のデバイスが通信許可された装置であることを報告する第5のステップと、第5のステップの後に、前記第1のデバイスと前記第2のデバイスの通信を開始する第6のステップとからなる通信認証方法。

【請求項10】 通信認証装置と第1のデバイスと第2のデバイスとがそれぞれ無線通信で接続され、前記第1のデバイスと前記第2のデバイスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記通信認証装置から前記第2のデバイスに対して情報を要求する第1のステップと、第1のステップの後に、前記第2のデバイスから前記通信認証装置に対して、どのような種類の前記第1のデバイスが利用可能であるか問い合わせる第2のステップと、第2のステップの後に、前記通信認証装置が、利用可能な前記第1のデバイスを検索する第3のステップと、第3のステップの後に、前記第1の

バスの存在情報を通知する第4のステップと、第4のステップの後に、前記通信認証装置が前記第1のバスの存在を確認した結果を前記第2のバスに報告する第5のステップと、第5のステップの後に、前記第1のバスと前記第2のバスの通信を開始する第6のステップとからなる通信認証方法。

【請求項11】 通信認証装置と第1のバスと第2のバスとがそれぞれ無線通信で接続され、前記第1のバスと前記第2のバスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記通信認証装置から前記第2のバスに対して情報を要求する第1のステップと、第1のステップの後に、前記第2のバスから前記通信認証装置に対して、どのような種類の前記第1のバスが登録されているかを問い合わせる第2のステップと、第2のステップの後に、前記通信認証装置が、利用可能な前記第1のバスを検索する第3のステップと、前記第1のバスから前記通信認証装置に対して、前記第1のバスのアドレス情報又はパスワード情報を送信する第4のステップと、第4のステップの後に、前記通信認証装置が前記第1のバスを認証する第5のステップと、第5のステップの後に、前記通信認証装置から前記第2のバスに対して、使用する前記第1のバスのアドレス情報又はパスワード情報を送信する第6のステップと、第6のステップの後に、前記第1のバスと前記第2のバスの通信を開始する第7のステップとからなる通信認証方法。

【請求項12】 通信認証装置と第1のバスと第2のバスとがそれぞれ無線通信で接続され、前記第1のバスと前記第2のバスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記第2のバスから前記通信認証装置に対して情報を要求する第1のステップと、第1のステップの後に、前記通信認証装置から前記第2のバスに対して前記通信認証装置が記憶管理している前記第1のバスに関する情報を含む回答通知を送信する第2のステップと、第2のステップの後に、前記第2のバスから特定された前記第1のバスに対して確認要求を行う第3のステップと、第3のステップの後に、前記第1のバスから前記第2のバスに対して、確認結果を送信する第4のステップとからなる通信認証方法。

【請求項13】 前記認証手段を、使用者個人を特定することが可能な生体情報を読み取って認証する生体情報認証手段とし、前記記憶手段には、使用者個人特有の生体情報を記憶することを特徴とする請求項1に記載の通信認証装置。

【請求項14】 通信認証装置と第1のバスと第2のバスとがそれぞれ無線通信で接続され、前記第2のバスには外部装置が接続され、前記第1のバスと前記第2のバスとの間の通信を前記通信認証装

置で認証する通信認証方法であって、前記第1のバスから前記第2のバスに対して接続要求を出す第1のステップと、第1のステップの後に、前記第2のバスが前記第1のバスへ接続してよいかどうかを、前記第2のバスから前記通信認証装置に対して問い合わせる第2のステップと、第2のステップの後に、前記第1のバスの所有者が前記通信認証装置の所有者であり、かつ前記通信認証装置が所有者本人の持ち物である証明を、前記通信認証装置に搭載された生体情報認証手段を用いて認証する第3のステップと、第3のステップの後に、前記第3のステップの認証結果が正しければ、前記認証結果を前記通信認証装置から前記第2のバスを経由して、前記第2のバスに接続されている外部装置に送信する第4のステップと、第4のステップの後に、前記外部装置から前記第2のバスを経由して、前記通信認証装置へ通信許可通知を送信する第5のステップと、第5のステップの後に、前記第1のバスと前記第2のバスの通信を開始する第6のステップとからなることを特徴とする通信認証方法。

【請求項15】 前記第5のステップの後に、前記第2のバスと通信を開始するのが、前記第2のバスに接続された第3のバスであることを特徴とする請求項14に記載の通信認証方法。

【請求項16】 第1のバスと第2のバスが無線または有線接続され、通信認証装置と第2のバスとが無線通信で接続され、前記第2のバスには外部装置が接続され、前記第1のバスと前記第2のバスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記第1のバスから前記第2のバスに対して接続要求を出す第1のステップと、第1のステップの後に、前記第2のバスが前記第1のバスへ接続してよいかどうかを、前記第2のバスから前記通信認証装置に対して問い合わせる第2のステップと、第2のステップの後に、前記第1のバスの所有者が前記通信認証装置の所有者であり、かつ前記通信認証装置が所有者本人の持ち物である証明を、前記通信認証装置に搭載された生体情報認証手段を用いて認証する第3のステップと、第3のステップの後に、前記第3のステップの認証結果が正しければ、前記認証結果を前記通信認証装置から前記第2のバスを経由して、前記第2のバスに接続されている外部装置に送信する第4のステップと、第4のステップの後に、前記外部装置から前記第2のバスに対して、データを送信する第5のステップとからなることを特徴とする通信認証方法。

【請求項17】 通信認証装置と第2のバスとが無線通信で接続され、前記第2のバスには外部装置が接続され、前記第2のバスの動作制御を前記外部装置から行う許可を前記通信認証装置で認証する通信認証方法であって、前記通信認証装置が所有者本人の持ち物

である証明を、前記通信認証装置に搭載された生体情報認証手段を用いて認証する第1のステップと、第1のステップの後に、前記第1のステップの認証結果が正しければ、前記認証結果を前記通信認証装置から前記第2のデバイスを経由して、前記第2のデバイスに接続されている外部装置に送信する第2のステップと、第2のステップの後に、前記外部装置から前記第2のデバイスに対して許可データを送信する第3のステップと、第3のステップの後に、前記外部装置から前記第2のデバイスに対して送信された許可データに基づいて前記第2のデバイスが動作を開始する第4のステップとからなることを特徴とする通信認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、携帯端末、携帯電話、パーソナルコンピュータ、デジタル音響機器等のデバイス間の無線接続を認証する通信認証装置及び通信認証方法に関する。

【0002】

【従来の技術】近年、インターネットの普及やマルチメディアの発展にともなう、情報ネットワーク技術が飛躍的に進歩し、携帯端末、携帯電話、パーソナルコンピュータ、これらの周辺機器、又はデジタル音響機器等の情報通信装置や情報家電装置が、パーソナルコンピュータを中心としたネットワーク上で利用されることが多くなっている。これらの情報通信装置や情報家電装置は、携帯性を重視する必要性から、機能を必要最小限にとどめ、それぞれの機器をコードを用いて接続することで、機能向上を図ったり、データ転送を行っている。しかし、コードを用いた接続では、コードを紛失したり、探し回らなければならない不都合を生じたり、コード配線による煩わしさがあった。このような状況の中で、ワイヤレスによって接続可能な機器が提案され、多くの企業は社内での無線通信によるデータ共有を推進し始め、個人生活においても、家庭内での情報家電装置間のワイヤレス化や、ショッピングなど屋外における生活シーンにおいても携帯端末による電子決済や情報収集手段として、さまざまな携帯型ワイヤレス通信装置が提案されてきている。比較的近距离の無線通信の手段としては、現在一般使用段階にある無線LANと、将来的に普及が見込まれているブルートゥースとがある。しかし、どちらの通信方法も、ケーブルを接続しなければ、ほぼ100%他者にデータを盗まれない有線通信と比較すると、無線通信は比較的広範囲の空中を電波が飛び回ることから、無線通信機器の機密管理技術や暗号化技術は必須の課題である。無線LANは、有線LANの規格であるIEEE802.11を拡張したものであり、有線LANの主流であるイーサネット（登録商標）（10baseイーサネット（登録商標））のケーブルを電波で置き換えたものである。よって、イーサネット（登録商標）で

はネットワークに接続されたパソコンや機器を識別するために、それぞれ「IPアドレス」という個別の番号を割り振らなければならない。これは無線LANでも同様であり、無線通信を行うパソコンはIPアドレスを持たなければならない。このIPアドレスをネットワーク機器側から自動的に割り振るようにしたのが、ダイヤルアップルータなどに搭載されている「DHCPサーバ機能」であり、現在汎用的に利用されているOSには、DHCPサーバが発行するアドレスを自動で受け入れるDHCPクライアント機能を装備している。ルータ機能を持つアクセスポイントを使う場合は、これを有効にしておき、IPアドレスの設定をパソコンに任せる方法と、IPアドレスを手動で設定する方法とがある。また、イーサネット（登録商標）につながるコンピュータのイーサネット（登録商標）ボードには、MACアドレス（Media Access Control Address）という固有の物理アドレスが付いている。MACアドレスはイーサネット（登録商標）であれば6バイト長で、先頭の3バイトはベンダコードとしてIEEE（米国電気電子学会）が管理/割り当てを行なっている。残り3バイトは各ベンダで独自に重複しないように管理しているコードなので、結果として、世界中で同じ物理アドレスを持つイーサネット（登録商標）ボードは存在せず、すべて異なるアドレスが割り当てられている。イーサネット（登録商標）ではこのアドレスを元にしてフレームの送受信を行っている。MACアドレスはハードウェアアドレスとも呼ばれ、TCP/IPのネットワークに接続する場合、ネットワーク管理者が前もってTCP/IPの設定をする必要がある。よって、無線LAN接続が可能な機器を、無線通信有効範囲内に持ち込んだとしても、MACアドレスやTCP/IPの設定等が必要となるので、個人の無線LAN環境においては、使用者本人が把握することになり、会社等の無線LAN環境においては、ネットワーク管理者の管理下に置かれるので、機密保持手段のひとつとなり得る。一方ブルートゥースが対象とするモバイル端末とは、業務用端末から消費マ製品に至るまで幅広いモバイル端末を想定しており、複雑な装置やOS上の設定の必要がなく、誰もが簡単に利用できるものとなっている。例を挙げると、ブルートゥースに対応したモバイル端末なら、近くにデータ・アクセス・ポイント（インターネット・ステーション）さえあればケーブルなしでインターネット接続が可能となったり、ブルートゥース搭載の携帯電話なら、パソコンの近くに置いておくだけでワイヤレス・モデムとしても利用可能となる。また、会議室にブルートゥース対応機器を持ち込むだけで、同席者のブルートゥース対応機器と自動的にピアツーピア・ネットワークを構成し、データやファイルなど互いの情報を必要に応じて無線で手軽に交換可能となり、個人使用としては、帰宅後入室と同時に手持ちのモバイル端末と自宅のパソコン

ンや、その他のハンドヘルド機器、携帯電話などの間でブルートゥース接続が自動的にされ、スケジュールやアドレス帳のようなファイルも自動的に同期化できる。ブルートゥース規格は、データリンク層でデバイス認証と暗号セキュリティ・サービスを定義しているので、ブルートゥースの通信接続方式のセキュリティ面での課題は、安全性を確保できないセキュリティ・プロトコルを組み込んだ装置や、全くセキュリティ・プロトコルを組み込んでいない装置との無線接続である。また、セキュリティのためにグループ外の装置を受け付けられない無線ネットワークであると、新たな装置が、その無線通信エリア内に入ってきて通信が始まらないというブルートゥース本来の趣旨に反する形態になってしまう。また、この新たな機器をブルートゥース機器として使用するための登録作業に複雑なIDやパスワードが必要になってくるという結果になる。また、現在のパスワードの一般的な運用方法は、仕事の形態においては、仕事用のノートパソコン等をモバイルパソコンとして、オフィスや自宅以外に持ち出している。そのため、機密性の高いデータを保存しているパソコンは、その内部データの機密保持の手段として、電源立ち上げ時にパスワードを要求してくる「BIOSによるパワーオン・パスワード」や、ファイルを読む時にパスワードを要求してくる「ハードディスク・パスワード」や、専用の暗号化ソフトを利用したファイル暗号化など様々な方法をとっている。つまり、複数のパスワードを使用するのであるが、パスワードの性格として、使用者に関係のある誕生日や電話番号等、他人が容易に知り得る文字列は通常使わない。実際のところは、使用者とは何の関係もない無意味な長い文字列を覚えておいて、機密解除作業ごとに異なるパスワードを入力するという作業となっている。このように複雑なパスワードであると、使用者は忘れないために手帳等にメモを取る場合が多く、パスワード自体を機密管理しなければならないという本来の仕事から離れた手間のかかる作業に時間や神経を使っているのが実状である。

#### 【0003】

【発明が解決しようとする課題】将来的に普及が見込まれているブルートゥース方式のモバイル端末や家電装置などは、業務用端末からコンシューマ製品、一般家電製品に至るまで幅広い製品群を想定しており、複雑な装置やOS上の設定の必要なく誰もが簡単に利用できるものとなっているので、例えば、無線通信エリア内に持ち込んだモバイル端末の通信環境下では、認証していない他人のモバイル端末が、エリア内のマスターである使用者の意に反して勝手にネットワークに接続されていたり、通信中のデータ内にある機密情報や個人情報などを他人に故意に盗み見られる可能性があり、このような無防備な無線通信エリアでは、データ通信を開始する時に通信装置間での通信方式や装置の認証が必要である。この認証方法としては、パスワード入力による認証があるが、操作

が容易でないと、「誰もが簡単に利用できる」ことがメ리트であるブルートゥース方式の装置の利便性を損ねてしまう結果となる。そこで、ある一定の条件のもとでは容易にネットワークを構築し、なおかつセキュリティも強固な通信認証方法が求められている。

【0004】そこで本発明は、さまざまに構成されたブルートゥース方式のモバイル端末や家電装置と、無線通信で接続され、ブルートゥース方式のモバイル端末や家電装置が「データ通信」を開始する前に、個々の装置がその無線通信エリア内での接続許可されたものかどうか認証する通信認証装置を提供することを目的とする。

#### 【0005】

【課題を解決するための手段】請求項1記載の本発明の通信認証装置は、携帯端末、携帯電話、パーソナルコンピュータ、デジタル音響機器等のデバイス間の無線接続を認証する通信認証装置であって、それぞれの前記デバイスと無線接続を行う通信手段と、前記デバイス間のデータの送信又は受信を可能とするか否かを判別する認証手段と、前記通信手段と前記認証手段とを制御する制御手段と、前記制御手段で使用する認証制御用データを記憶する記憶手段とを有することを特徴とする。請求項2記載の本発明は、請求項1に記載の通信認証装置において、前記記憶手段には、使用者の氏名、生年月日、電話番号、電子メールアドレス、免許証番号など複数の実際の個人データをパスワードとして記憶することを特徴とする。請求項3記載の本発明は、請求項1に記載の通信認証装置において、前記記憶手段の内部メモリに管理対象となるデバイスの情報を入力する入力手段と、前記ネットワークの通信状態や前記入力手段からの入力情報を表示する表示手段とを有することを特徴とする。請求項4記載の本発明は、請求項1に記載の通信認証装置において、前記制御手段に接続され、外部から起動ができる起動手段を備えたことを特徴とする。請求項5記載の本発明は、請求項1に記載の通信認証装置において、前記制御手段に接続され、あらかじめ決めた位置でのみ制御動作を行うための位置情報検出手段を備えたことを特徴とする。請求項6記載の本発明は、請求項1に記載の通信認証装置において、前記制御手段に接続され、使用者が設定した時刻や一定時間のみ制御手段からの通信命令や認証命令を動作させるタイマー手段を備えたことを特徴とする。請求項7記載の本発明の通信認証方法は、通信認証装置と第1のデバイスと第2のデバイスとがそれぞれ無線通信で接続され、前記第1のデバイスと前記第2のデバイスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記第1のデバイスから前記第2のデバイスに対して接続要求を出す第1のステップと、第1のステップの後に、前記第2のデバイスが前記第1のデバイスへ接続してよいかどうかを、前記第2のデバイスから前記通信認証装置に対して問い合わせる第2のステップと、第2のステップの後に、前記通信認証



装置が前記第1のデバイスの存在を確認する第3のステップと、第3のステップの後に、前記第1のデバイスから前記通信認証装置に対して前記第1のデバイスの存在情報を通知する第4のステップと、第4のステップの後に、前記通信認証装置が前記第1のデバイスの存在を確認した結果を、前記通信認証装置から前記第2のデバイスに対して報告する第5のステップと、第5のステップの後に、前記第1のデバイスと前記第2のデバイスの通信を開始する第6のステップとからなることを特徴とする。請求項8記載の本発明の通信認証方法は、通信認証装置と第1のデバイスと第2のデバイスとがそれぞれ無線通信で接続され、前記第1のデバイスと前記第2のデバイスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記第1のデバイスから前記第2のデバイスに対して接続要求を出す第1のステップと、第1のステップの後に、前記第2のデバイスが前記第1のデバイスへ接続してよいかどうかを、前記第2のデバイスから前記通信認証装置に対して問い合わせる第2のステップと、第2のステップの後に、前記通信認証装置と前記第1のデバイスの間で、前記第1のデバイスのアドレス情報又はパスワード情報を送受信することによって前記第1のデバイスを認証する第3のステップと、第3のステップの後に、前記通信認証装置から前記第2のデバイスに対して前記第1のデバイスが通信許可された装置であることを報告する第4のステップと、第4のステップの後に、前記第1のデバイスと前記第2のデバイスの通信を開始する第5のステップとからなることを特徴とする。請求項9記載の本発明の通信認証方法は、通信認証装置と第1のデバイスと第2のデバイスとがそれぞれ無線通信で接続され、前記第1のデバイスと前記第2のデバイスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記第1のデバイスから前記第2のデバイスに対して接続要求を出す第1のステップと、第1のステップの後に、前記第2のデバイスが前記第1のデバイスへ接続してよいかどうかを、前記第2のデバイスから前記通信認証装置に対して問い合わせる第2のステップと、第2のステップの後に、前記通信認証装置と前記第2のデバイスの間で、前記第2のデバイスのアドレス情報又はパスワード情報を送受信することによって前記第2のデバイスを認証する第3のステップと、第3のステップの後に、前記通信認証装置と前記第1のデバイスの間で、前記第1のデバイスのアドレス情報又はパスワード情報を送受信することによって前記第1のデバイスを認証する第4のステップと、第4のステップの後に、前記通信認証装置から前記第2のデバイスに対して、前記第1のデバイスが通信許可された装置であることを報告する第5のステップと、第5のステップの後に、前記第1のデバイスと前記第2のデバイスの通信を開始する第6のステップとからなることを特徴とする。請求項10記載の本発明の通信認証方法は、通信認

証装置と第1のデバイスと第2のデバイスとがそれぞれ無線通信で接続され、前記第1のデバイスと前記第2のデバイスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記通信認証装置から前記第2のデバイスに対して情報を要求する第1のステップと、第1のステップの後に、前記第2のデバイスから前記通信認証装置に対して、どのような種類の前記第1のデバイスが利用可能であるか問い合わせる第2のステップと、第2のステップの後に、前記通信認証装置が、利用可能な前記第1のデバイスを検索する第3のステップと、第3のステップの後に、前記第1のデバイスから前記通信認証装置に対して前記第1のデバイスの存在情報を通知する第4のステップと、第4のステップの後に、前記通信認証装置が前記第1のデバイスの存在を確認した結果を前記第2のデバイスに報告する第5のステップと、第5のステップの後に、前記第1のデバイスと前記第2のデバイスの通信を開始する第6のステップとからなることを特徴とする。請求項11記載の本発明の通信認証方法は、通信認証装置と第1のデバイスと第2のデバイスとがそれぞれ無線通信で接続され、前記第1のデバイスと前記第2のデバイスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記通信認証装置から前記第2のデバイスに対して情報を要求する第1のステップと、第1のステップの後に、前記第2のデバイスから前記通信認証装置に対して、どのような種類の前記第1のデバイスが登録されているかを問い合わせる第2のステップと、第2のステップの後に、前記通信認証装置が、利用可能な前記第1のデバイスを検索する第3のステップと、前記第1のデバイスから前記通信認証装置に対して、前記第1のデバイスのアドレス情報又はパスワード情報を送信する第4のステップと、第4のステップの後に、前記通信認証装置が前記第1のデバイスを認証する第5のステップと、第5のステップの後に、前記通信認証装置から前記第2のデバイスに対して、使用する前記第1のデバイスのアドレス情報又はパスワード情報を送信する第6のステップと、第6のステップの後に、前記第1のデバイスと前記第2のデバイスの通信を開始する第7のステップとからなることを特徴とする。請求項12記載の本発明の通信認証方法は、通信認証装置と第1のデバイスと第2のデバイスとがそれぞれ無線通信で接続され、前記第1のデバイスと前記第2のデバイスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記第2のデバイスから前記通信認証装置に対して情報を要求する第1のステップと、第1のステップの後に、前記通信認証装置から前記第2のデバイスに対して前記通信認証装置が記憶管理している前記第1のデバイスに関する情報を含む回答通知を送信する第2のステップと、第2のステップの後に、前記第2のデバイスから特定された前記第1のデバイスに対して確認要求を行う第3のステップと、第3のステップの後



に、前記第1のデバイスから前記第2のデバイスに対して、確認結果を送信する第4のステップとからなることを特徴とする。請求項13記載の本発明は、請求項1に記載の通信認証装置において、前記認証手段を、使用者個人を特定することが可能な生体情報を読み取って認証する生体情報認証手段とし、前記記憶手段には、使用者個人特有の生体情報を記憶することを特徴とする。請求項14記載の本発明の通信認証方法は、通信認証装置と第1のデバイスと第2のデバイスとがそれぞれ無線通信で接続され、前記第2のデバイスには外部装置が接続され、前記第1のデバイスと前記第2のデバイスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記第1のデバイスから前記第2のデバイスに対して接続要求を出す第1のステップと、第1のステップの後に、前記第2のデバイスが前記第1のデバイスへ接続してよいかどうかを、前記第2のデバイスから前記通信認証装置に対して問い合わせる第2のステップと、第2のステップの後に、前記第1のデバイスの所有者が前記通信認証装置の所有者であり、かつ前記通信認証装置が所有者本人の持ち物である証明を、前記通信認証装置に搭載された生体情報認証手段を用いて認証する第3のステップと、第3のステップの後に、前記第3のステップの認証結果が正しければ、前記認証結果を前記通信認証装置から前記第2のデバイスを経由して、前記第2のデバイスに接続されている外部装置に送信する第4のステップと、第4のステップの後に、前記外部装置から前記第2のデバイスを経由して、前記通信認証装置へ通信許可通知を送信する第5のステップと、第5のステップの後に前記第1のデバイスと前記第2のデバイスの通信を開始する第6のステップとからなることを特徴とする。請求項15記載の本発明の通信認証方法は、請求項14に記載の通信認証方法において、前記第5のステップの後に、前記第2のデバイスと通信を開始するのが、前記第2のデバイスに接続された第3のデバイスであることを特徴とする。請求項16記載の本発明の通信認証方法は、第1のデバイスと第2のデバイスが無線または有線接続され、通信認証装置と第2のデバイスとが無線通信で接続され、前記第2のデバイスには外部装置が接続され、前記第1のデバイスと前記第2のデバイスとの間の通信を前記通信認証装置で認証する通信認証方法であって、前記第1のデバイスから前記第2のデバイスに対して接続要求を出す第1のステップと、第1のステップの後に、前記第2のデバイスが前記第1のデバイスへ接続してよいかどうかを、前記第2のデバイスから前記通信認証装置に対して問い合わせる第2のステップと、第2のステップの後に、前記第1のデバイスの所有者が前記通信認証装置の所有者であり、かつ前記通信認証装置が所有者本人の持ち物である証明を、前記通信認証装置に搭載された生体情報認証手段を用いて認証する第3のステップと、第3のステップの後に、前記第3のステップ

の認証結果が正しければ、前記認証結果を前記通信認証装置から前記第2のデバイスを経由して、前記第2のデバイスに接続されている外部装置に送信する第4のステップと、第4のステップの後に、前記外部装置から前記第2のデバイスに対して、データを送信する第5のステップとからなることを特徴とする。請求項17記載の本発明の通信認証方法は、通信認証装置と第2のデバイスとが無線通信で接続され、前記第2のデバイスには外部装置が接続され、前記第2のデバイスの動作制御を前記外部装置から行う許可を前記通信認証装置で認証する通信認証方法であって、前記通信認証装置が所有者本人の持ち物である証明を、前記通信認証装置に搭載された生体情報認証手段を用いて認証する第1のステップと、第1のステップの後に、前記第1のステップの認証結果が正しければ、前記認証結果を前記通信認証装置から前記第2のデバイスを経由して、前記第2のデバイスに接続されている外部装置に送信する第2のステップと、第2のステップの後に、前記外部装置から前記第2のデバイスに対して許可データを送信する第3のステップと、第3のステップの後に、前記外部装置から前記第2のデバイスに対して送信された許可データに基づいて前記第2のデバイスが動作を開始する第4のステップとからなることを特徴とする。

#### 【0006】

【発明の実施の形態】本発明の第1の実施の形態による通信認証装置は、それぞれのデバイスと無線接続を行う通信手段と、デバイス間のデータの送信又は受信を可能とするか否かを判別する認証手段と、通信手段と認証手段とを制御する制御手段と、制御手段で使用する認証制御用データを記憶する記憶手段とを有するものである。本実施の形態によれば、無線通信が可能なエリア内にある2台以上の通信装置とは別に存在する通信認証装置によって、エリア内にある2台以上の通信装置を互いに「データ通信」可能とするか否かの制御をすることができ、従って、あらかじめ通信認証装置に認証制御用データが記憶されていれば、この通信認証装置をエリア内に持ち込むことにより、通信認証装置内部の記憶手段に記憶された認証制御用データに登録されている通信装置を接続して使用可能とすることができる。

【0007】本発明の第2の実施の形態は、第1の実施の形態による通信認証装置において、記憶手段には、使用者の氏名、生年月日、電話番号、電子メールアドレス、免許証番号など複数の実際の個人データをパスワードとして記憶するものである。本実施の形態によれば、使用者自身に由縁のある氏名、生年月日、電話番号、電子メールアドレス、免許証番号等の情報をパスワードとして登録するので、忘却する危険性が少なく、パスワードを書き留める必要がない。

【0008】本発明の第3の実施の形態は、第1の実施の形態による通信認証装置において、記憶手段の内部メ

モリに管理対象となるデバイスの情報を入力する入力手段と、ネットワークの通信状態や入力手段からの入力情報を表示する表示手段とを有するものである。本実施の形態によれば、無線通信が可能なエリア内にある2台以上のデバイスとは別に存在する通信認証装置によって、エリア内にある2台以上のデバイスを互いに「データ通信」可能とするか否かの制御をすることができる。従って、あらかじめ通信認証装置に認証制御用データが記憶されていれば、この通信認証装置をエリア内に持ち込むことにより、通信認証装置内部の記憶手段に記憶された認証制御用データに登録されているデバイスを接続して使用可能とすることができる。さらに、入力手段として釦や表示手段として表示窓を設けることにより、移動先の通信エリアでの急な認証作業が可能となる。

【0009】本発明の第4の実施の形態は、第1の実施の形態による通信認証装置において、制御手段に接続され、外部から起動ができる起動手段を備えたものである。本実施の形態によれば、据え置かれた通信認証装置の場合でも、使用者の入室を検知したり、鍵の挿入を検知したり、その他装置の起動に同期して、通信認証装置を起動できるので、通信認証装置の存在を気にすることなく快適にセキュリティを保持できる。従って、例えば自動車等にキーレスエントリーで搭乗した時や、鍵を使用してエンジンスタートした時に、通信認証装置を起動して携帯電話とカーナビゲーション装置をブルートゥースで接続して通信をし、携帯電話から基地局経由で地図情報を受信し、カーナビゲーション装置に送信したりできる。

【0010】本発明の第5の実施の形態は、第1の実施の形態による通信認証装置において、制御手段に接続され、あらかじめ決めた位置でのみ制御動作を行うための位置情報検出手段を備えたものである。本実施の形態によれば、通信認証装置の内部の位置情報検出手段により、使用者があらかじめ設定した地球上の座標に居る場合のみ各デバイスの使用が可能となる。従って、決まった場所でのみ通信認証を行うので、強固なセキュリティを保持できる。

【0011】本発明の第6の実施の形態は、第1の実施の形態による通信認証装置において、制御手段に接続され、使用者が設定した時刻や一定時間のみ制御手段からの通信命令や認証命令を動作させるタイマー手段を備えたものである。本実施の形態によれば、通信認証装置の内部のタイマー手段により、使用者があらかじめ設定した時刻や、使用者が設定した時間経過後、あるいは使用者が設定した時間内で各デバイスの使用が可能となる。従って、第三者の通信認証装置の無断使用による通信認証を防止できる。

【0012】本発明の第7の実施の形態による通信認証方法は、第1のデバイスから第2のデバイスに対して接続要求を出す第1のステップと、第1のステップの後

に、第2のデバイスが第1のデバイスへ接続してよいかどうかを、第2のデバイスから通信認証装置に対して問い合わせる第2のステップと、第2のステップの後に、通信認証装置が第1のデバイスの存在を確認する第3のステップと、第3のステップの後に、第1のデバイスから通信認証装置に対して第1のデバイスの存在情報を通知する第4のステップと、第4のステップの後に、通信認証装置が第1のデバイスの存在を確認した結果を、通信認証装置から第2のデバイスに対して報告する第5のステップと、第5のステップの後に、第1のデバイスと第2のデバイスの通信を開始する第6のステップとからなるものである。本実施の形態によれば、通信認証装置を無線通信エリア内に持ち込むことにより、はじめて第1のデバイスと第2のデバイスが、通信認証装置が介在することによってデータ通信を開始するので、第3者からの勝手なアクセスによる接続での機密データの流出が生じない。

【0013】本発明の第8の実施の形態による通信認証方法は、第1のデバイスから第2のデバイスに対して接続要求を出す第1のステップと、第1のステップの後に、第2のデバイスが第1のデバイスへ接続してよいかどうかを、第2のデバイスから通信認証装置に対して問い合わせる第2のステップと、第2のステップの後に、通信認証装置と第1のデバイスの間で、第1のデバイスのアドレス情報又はパスワード情報を送受信することによって第1のデバイスを認証する第3のステップと、第3のステップの後に、通信認証装置から第2のデバイスに対して第1のデバイスが通信許可された装置であることを報告する第4のステップと、第4のステップの後に、第1のデバイスと第2のデバイスの通信を開始する第5のステップとからなるものである。本実施の形態によれば、通信認証装置を無線通信エリア内に持ち込み、第1のデバイスをパスワード等の認証手段を用いることにより、はじめて第1のデバイスと第2のデバイスがデータ通信を開始するので、第3者からの勝手なアクセスによる接続での機密データの流出が生じない。

【0014】本発明の第9の実施の形態による通信認証方法は、第1のデバイスから第2のデバイスに対して接続要求を出す第1のステップと、第1のステップの後に、第2のデバイスが第1のデバイスへ接続してよいかどうかを、第2のデバイスから通信認証装置に対して問い合わせる第2のステップと、第2のステップの後に、通信認証装置と第2のデバイスの間で、第2のデバイスのアドレス情報又はパスワード情報を送受信することによって第2のデバイスを認証する第3のステップと、第3のステップの後に、通信認証装置と第1のデバイスの間で、第1のデバイスのアドレス情報又はパスワード情報を送受信することによって第1のデバイスを認証する第4のステップと、第4のステップの後に、通信認証装置から第2のデバイスに対して、第1のデバイスが通信

許可された装置であることを報告する第5のステップと、第5のステップの後に、第1のデバイスと第2のデバイスの通信を開始する第6のステップとからなるものである。本実施の形態によれば、通信認証装置を無線通信エリア内に持ち込み、第2のデバイスをパスワード等の認証手段を用いることにより、はじめて第1のデバイスと第2のデバイスがデータ通信を開始するので、第3者からの勝手なアクセスによる接続での機密データの流出が生じない。

【0015】本発明の第10の実施の形態による通信認証方法は、通信認証装置から第2のデバイスに対して情報を要求する第1のステップと、第1のステップの後に、第2のデバイスから通信認証装置に対して、どのような種類の第1のデバイスが利用可能であるか問い合わせる第2のステップと、第2のステップの後に、通信認証装置が、利用可能な第1のデバイスを検索する第3のステップと、第3のステップの後に、第1のデバイスから通信認証装置に対して第1のデバイスの存在情報を通知する第4のステップと、第4のステップの後に、通信認証装置が第1のデバイスの存在を確認した結果を第2のデバイスに報告する第5のステップと、第5のステップの後に、第1のデバイスと第2のデバイスの通信を開始する第6のステップとからなるものである。本実施の形態によれば、通信認証装置を無線通信エリア内に持ち込み、第2のデバイスの使用により第1のデバイスと接続すべき第2のデバイスを認証し、その認証情報を第1のデバイスに送信することにより、はじめて第1のデバイスと第2のデバイスがデータ通信を開始するので、第3者からの勝手なアクセスによる接続での機密データの流出が生じない。

【0016】本発明の第11の実施の形態による通信認証方法は、通信認証装置から第2のデバイスに対して情報を要求する第1のステップと、第1のステップの後に、第2のデバイスから通信認証装置に対して、どのような種類の第1のデバイスが登録されているかを問い合わせる第2のステップと、第2のステップの後に、通信認証装置が、利用可能な第1のデバイスを検索する第3のステップと、第1のデバイスから通信認証装置に対して、第1のデバイスのアドレス情報又はパスワード情報を送信する第4のステップと、第4のステップの後に、通信認証装置が第1のデバイスを認証する第5のステップと、第5のステップの後に、通信認証装置から第2のデバイスに対して、使用する第1のデバイスのアドレス情報又はパスワード情報を送信する第6のステップと、第6のステップの後に、第1のデバイスと第2のデバイスの通信を開始する第7のステップとからなるものである。本実施の形態によれば、通信認証装置を無線通信エリア内に持ち込み、まず第1のデバイスを確定し、次に第2のデバイスの使用により第1のデバイスと接続すべき第2のデバイスを認証し、その認証情報を第1のデバ

イスに送信することにより、はじめて第1のデバイスと第2のデバイスがデータ通信を開始するので、第3者からの勝手なアクセスによる接続での機密データの流出が生じない。

【0017】本発明の第12の実施の形態による通信認証方法は、第2のデバイスから通信認証装置に対して情報を要求する第1のステップと、第1のステップの後に、通信認証装置から第2のデバイスに対して通信認証装置が記憶管理している第1のデバイスに関する情報を含む回答通知を送信する第2のステップと、第2のステップの後に、第2のデバイスから特定された第1のデバイスに対して確認要求を行う第3のステップと、第3のステップの後に、第1のデバイスから第2のデバイスに対して、確認結果を送信する第4のステップとからなるものである。本実施の形態によれば、通信認証装置を無線通信エリア内に持ち込み、第1のデバイスと第2のデバイスを認証した後、第2のデバイスから第1のデバイスに送信したデータの正誤を第1のデバイスの使用者が確認し、第2のデバイスに結果報告することにより、はじめて第2のデバイスが別の通信回線を使用して第1のデバイスから送られてきたデータを転送し計算するので、クレジットカードや金額情報等の個人情報、第3者からの勝手なアクセスによる接続によって外部に流出しない。

【0018】本発明の第13の実施の形態は、第1の実施の形態による通信認証装置において、認証手段を、使用者個人を特定することが可能な生体情報を読み取って認証する生体情報認証手段とし、記憶手段には、使用者個人特有の生体情報を記憶するものである。本実施の形態によれば、使用者自身を確定する人物認証に、使用者本人の指紋や角膜や遺伝子などの生体情報を用いて認証するため、通信認証装置の所有者や、通信認証装置を含むシステムの所有者と、現在の使用者が同一人物である確証がより正確に取れる。また、ほぼ100%の確立で同一の生体情報は存在しないため、使用者の特定精度を向上するためのパスワード等の認証キーを複数必要なくなり、結果として使用者の認証操作が簡単になる。更に、認証対象が1つの生体情報であっても十分に個人を特定できるため、人物認証するための通信認証装置の小型化や、認証アルゴリズムの簡略化が容易に図れる。

【0019】本発明の第14の実施の形態による通信認証方法は、第1のデバイスから第2のデバイスに対して接続要求を出す第1のステップと、第1のステップの後に、第2のデバイスが第1のデバイスへ接続してよいかどうかを、第2のデバイスから通信認証装置に対して問い合わせる第2のステップと、第2のステップの後に、第1のデバイスの所有者が通信認証装置の所有者であり、かつ通信認証装置が所有者本人の持ち物である証明を、通信認証装置に搭載された生体情報認証手段を用いて認証する第3のステップと、第3のステップの後に、

第3のステップの認証結果が正しければ、認証結果を通信認証装置から第2のデバイスを経由して、第2のデバイスに接続されている外部装置に送信する第4のステップと、第4のステップの後に、外部装置から前記第2のデバイスを経由して、通信認証装置へ通信許可通知を送信する第5のステップと、第5のステップの後に、第1のデバイスと第2のデバイスの通信を開始する第6のステップとからなるものである。本実施の形態によれば、外部装置を含む第1と第2のデバイスと通信認証装置で構成されるシステム、あるいは第1のデバイスと通信認証装置が使用者自身の所有物であることの証明を、システム使用開始時に使用者自身の生体情報（指紋、角膜、遺伝子等）を用いて行うため、システム全体あるいは個々のデバイスからの機密情報の流出が生じない。また、第5のステップの後に、通信認証装置から第2のデバイスへ通信許可を送信し、その許可情報によって第1のデバイスと第2のデバイスの通信を開始するようにすれば、更に強固に通信の機密を保つことができる。なお、第5のステップにおける通信データの流れを第2のデバイスが監視しておいて、第2のデバイスから確実に通信許可が通信認証装置に送り出されたことを検出して、その検出結果をもって第1のデバイスと第2のデバイスの通信を開始する方法であっても十分に通信機密を保持できる。

【0020】本発明の第15の実施の形態による通信認証方法は、本発明の第14の実施の形態による通信認証方法において、第5のステップの後に、第2のデバイスと通信を開始するのが、第2のデバイスに接続された第3のデバイスであるものである。本実施の形態によれば、外部装置を含む第1と第2と第3デバイスと通信認証装置で構成されるシステム、あるいは第1のデバイスと通信認証装置が使用者自身の所有物であることの証明を、システム使用開始時に使用者自身の生体情報（指紋、角膜、遺伝子等）を用いて行うため、システム全体あるいは個々のデバイスからの機密情報の流出が生じない。また、第1のデバイスが機密性の高い操作系機器で、第3のデバイスは公共性の高い表示系機器というような自由度の高いシステムを構築できる。もちろん、第3のデバイスも個人専用機器であり、通信認証装置によってセキュリティをかけた装置であってもよい。

【0021】本発明の第16の実施の形態による通信認証方法は、第1のデバイスから第2のデバイスに対して接続要求を出す第1のステップと、第1のステップの後に、第2のデバイスが第1のデバイスへ接続してよいかどうかを、第2のデバイスから通信認証装置に対して問い合わせる第2のステップと、第2のステップの後に、第1のデバイスの所有者が通信認証装置の所有者であり、かつ通信認証装置が所有者本人の持ち物である証明を、通信認証装置に搭載された生体情報認証手段を用いて認証する第3のステップと、第3のステップの後に、

第3のステップの認証結果が正しければ、認証結果を前記通信認証装置から第2のデバイスを経由して、第2のデバイスに接続されている外部装置に送信する第4のステップと、第4のステップの後に、外部装置から前記第2のデバイスに対して、データを送信する第5のステップとからなるものである。本実施の形態によれば、外部装置を含む第1と第2のデバイスと通信認証装置で構成されるシステム、あるいは第1のデバイスと通信認証装置が使用者自身の所有物であることの証明を、システム使用開始時に使用者自身の生体情報（指紋、角膜、遺伝子等）を用いて行うため、システム全体あるいは個々のデバイスからの機密情報の流出が生じない。また、第1のデバイスが使用者自身の所有物であるという証明は、第1のデバイスと通信認証装置間で完了しているので、第2のデバイスや第2のデバイスに接続された外部装置内部で新たに個人情報等（クレジットカード番号等も含む）の機密データを照会する必要がない。

【0022】本発明の第17の実施の形態による通信認証方法は、通信認証装置が所有者本人の持ち物である証明を、前記通信認証装置に搭載された生体情報認証手段を用いて認証する第1のステップと、第1のステップの後に、第1のステップの認証結果が正しければ、認証結果を通信認証装置から第2のデバイスを経由して、第2のデバイスに接続されている外部装置に送信する第2のステップと、第2のステップの後に、外部装置から第2のデバイスに対して許可データを送信する第3のステップと、第3のステップの後に、外部装置から第2のデバイスに対して送信された許可データに基づいて第2のデバイスが動作を開始する第4のステップとからなるものである。本実施の形態によれば、外部装置を含む第2のデバイスと通信認証装置で構成されるシステム、あるいは第2のデバイスと通信認証装置、あるいは通信認証装置のみが使用者自身の所有物であることの証明を、システム使用開始時に使用者自身の生体情報（指紋、角膜、遺伝子等）を用いて行うため、システム全体あるいは個々のデバイスからの機密情報の流出が生じない。また、第2のデバイスが使用者自身の所有物であるという証明は、第2のデバイスと通信認証装置間で完了しているので、第2のデバイスや第2のデバイスに接続された外部装置内部で新たに個人情報等の機密データを照会する必要がない。

【0023】

【実施例】以下本発明の一実施例による通信認証装置について図面に基いて説明する。図1は一对のデバイスと最も簡略な通信認証装置の接続形態であり、通信認証装置を機能実現手段で表したブロック図である。まず、通信認証装置の基本機能について図1を用いて説明する。第1のデバイス2と、第2のデバイス3と、通信認証装置1とは、それぞれ通信回線8によって近距離無線通信で接続されている。近距離無線通信としては例えば

ブルートゥースを用いることができる。ここでブルートゥースは、2.4ギガヘルツのISMバンドで動作する無線通信技術である。図1において、通信認証装置1の通信手段4は、第1のデバイス2と、第2のデバイス3と、通信回線8を介して繋がっている。ここで、第1のデバイス2と第2のデバイス3とは、すぐに通信を開始するものではなく、通信認証装置1内部の記憶手段7に記憶された通信認証用データ（パスワードなど）や通信構成に従って認証手段5で認証が実行され、制御手段6によって通信手段4を制御してはじめて、第1のデバイス2と第2のデバイス3とのデータ通信が開始される。ここで通信認証装置1は、例えばICカードのように極めて軽量小型（薄型）の携帯できるものが好ましいが、据え置き型であってもよいし、同様の機能を追加機能として備えたパソコン、携帯電話、PHS、又はPDA等の携帯端末であってもよい。なお、通信機能を有する携帯端末の場合には、あらかじめ認証手段5を備えていなくても、認証手段5として必要なプログラムをサーバから通信回線を介してダウンロードして利用することもできる。例えばJava（登録商標）アプレットをWWWサーバからダウンロードして利用する。また、デバイス2およびデバイス3は通信機能を備えた装置であって、コンピュータ周辺機器であるキーボード、マウス、プリンター、イメージスキャナ、ターミナルアダプタや、モバイル機器であるデジタルカメラ、ナビゲーション装置、パームOSコンピュータや、一般家電機器をネットワーク対応にした情報家電装置や携帯電話など、通信機能によりさまざまに拡張される電気製品を含むデバイスである。なお、認証手段5は、使用者の指紋、角膜、遺伝子等の人体固有の生体情報を検出して認証を行うものであってもよい。

【0024】図2は、本発明の一実施例による通信認証装置を機能実現手段で表したブロック図であり、図1の通信認証装置1に追加機能として、表示手段10と入力手段11を設けたものである。表示手段10には通信状態や、入力手段11によって入力したパスワードなどを表示する。ここで、表示手段10としては、液晶表示が一般的であるが、プラズマやCRT等他の方式の表示でもよい。また、入力手段11としては、キーボードやテンキーボードが一般的であるが、タッチパネルや音声認識入力などでも実現できる。なお、認証手段5は、使用者の指紋、角膜、遺伝子等の人体固有の生体情報を検出して認証を行うものであってもよい。

【0025】図3は、本発明の一実施例による通信認証装置を機能実現手段で表したブロック図であり、さらに他の追加機能を含むものである。以下、特に追加機能について説明する。リムーバブルメモリ手段12は、前述の記憶手段7の内、記憶領域の全てか、又は一部の領域をリムーバブル領域で構成したもので、通信認証装置1以外の装置（例えばパソコン）で、認証用データを作成

することができる。ホストインターフェイス手段13は、外部にホストコンピュータ51を接続して記憶手段7内部の認証用データを追加、削除、訂正などのメンテナンスを行い、あるいは通信認証装置1自身が正常に動作しているか検査するなどのために設けたものである。起動手段14は、鍵52の挿入によって通信認証装置1をスタンバイ状態から起動動作させるものであり、特に携帯型の通信認証装置1である場合のバッテリー消費を考慮したものである。ここで鍵52は図3では接触挿入型で記載しているが、キーレスエントリーシステムなど非接触型鍵であってもよい。位置検出手段15は、通信認証装置1の位置を検出するものであり、位置情報によって通信認証装置1をスタンバイ状態から起動動作させたり、通信認証の開始や停止を行える。位置情報検出方法としては、GPSやPHSによる位置検出方法があるが、その他の方法であってもよい。また、位置検出地点の誤差除去ができるもの（D-GPS）であってもよい。タイマー手段16は、認証時間の設定、一定時間経過後の通信認証の開始又は停止などの用途で使用する。このタイマー手段16の設定によって、無人での通信認証装置1の使用や、通信認証装置1の所有者が不在の時間のセキュリティが確保できる。外部入力端子17は、通信認証装置1の外部にキーボード53等の入力装置を接続するための端子である。表示出力手段18は、通信認証装置1の外部に、モニター54などの表示手段を接続するためのものである。この表示出力手段18は、外部出力端子17と同様に、モニター54を接続することによって、設定変更などのメンテナンスを行うことができる。

【0026】本実施例では、制御手段における認証制御用データを記憶している記憶手段7の内、記憶領域の全てか、又は一部をリムーバブル領域で構成したリムーバブルメモリ手段12を備えることで、通信認証装置1の制御手段6における認証制御用データを、あらかじめ他のパーソナルコンピュータやパームOSコンピュータなどを用いて作成し、その後で通信認証装置1に格納することができる。従って、比較的容易にデバイスの登録や次回接続のネットワーク構成に合わせたデバイスの再構成などのメンテナンスができる。また本実施例では、通信手段4と認証手段5とを制御する制御手段6に接続され、記憶手段7の内部メモリへの管理対象デバイスの情報の入力や、ネットワークの通信状態を表示するためのホストコンピュータ51を接続するホストインターフェイス手段13を備えることで、通信認証装置1の制御手段6における認証制御用データを、有線又は無線で接続されたホストコンピュータ51を用いて作成したり、次回接続のネットワーク構成に合わせたデバイスの再構成などのメンテナンスや、通信状態が正常に動作できているか否かの確認を容易に行うことができる。また本実施例では、外部から接触又は非接触の起動ができる起動手段14を備えることで、据え置かれた通信認証装置1の



場合でも、使用者の入室を検知したり、鍵52の挿入を検知したり、その他装置の起動に同期して、通信認証装置1を起動できるので、通信認証装置1の存在を気にすることなく快適にセキュリティを保持できる。従って、例えば自動車等にキーレスエントリーで搭乗した時や、鍵を使用してエンジンスタートした時に、通信認証装置を起動して携帯電話とカーナビゲーション装置をBluetoothで接続して通信をし、携帯電話から基地局経由で地図情報を受信し、カーナビゲーション装置に送信することができる。

【0027】また本実施例では、位置情報検出手段15を備えているので、使用者があらかじめ設定した地球上の座標に居る場合のみ各デバイスの使用が可能となるように設定することができる。このように、決まった場所でのみ通信認証を行うことで、強固なセキュリティを保持できる。また本実施例では、使用者が設定した時刻や一定時間のみ制御手段6からの通信命令や認証命令を動作させるタイマー手段16を備えることで、使用者があらかじめ設定した時刻や、使用者が設定した時間経過後、あるいは使用者が設定した時間内で各デバイスの使用が可能となるように設定することができる。従って、第三者の通信認証装置1の無断使用による通信認証を防止できる。また本実施例では、外部入力装置53によって入力するための外部入力端子17を備えることで、ホストコンピュータの接続などの手間を掛けることなく、通信認証装置1の制御手段6における認証制御用データを入力して、記憶手段7の内部メモリに格納することができるので、比較的容易にデバイスの登録や次回接続のネットワーク構成に合わせたデバイスの再構成などのメンテナンスができる。従って、キーボード等を接続することによってのみ、通信認証装置の設定を変更できるので、第三者の通信認証装置の無断使用による通信認証を防止できる。また本実施例では、外部モニター54に表示するための表示出力端子18を備えることで、表示機能のない通信認証装置1に外部モニター54をつないで、通信状態確認時、デバイス登録時、メンテナンス時など使用者が必要な時のみ内部情報や通信形態の表示を行うことができる。従って、通信認証装置の管理者（使用者）のみ、内部に記憶されている通信形態や、現在の通信状況を閲覧できるので、第三者の通信認証装置の無断使用による通信認証を防止できる。なお、認証手段5は、使用者の指紋、角膜、遺伝子等の人体固有の生体情報を検出して認証を行うものであってもよい。なお、本実施例の通信認証装置1は、それぞれの機能を説明する上で、それぞれを別構成で説明したが、全ての手段を備えていてもよく、目的に応じた一部の手段を備えているものであってもよい。

【0028】図4と図5は、本発明の一実施例による通信認証方法を示すブロック図である。なお、以下の実施例で説明する通信認証装置1は、図1から図3で既に説

明した通信認証装置の構成を適用することができる。図4は第1のデバイス2がヘッドホンであり、第2のデバイス3がミュージックプレーヤーであって、両者の接続認証を通信認証装置1で行うものである。ヘッドホン2がミュージックプレーヤー3に接続要求を出すと（S401）、ミュージックプレーヤー3は通信認証装置1に対して接続してよいデバイスかどうか確認問い合わせをする（S402）。通信認証装置1はヘッドホン2の存在をチェックし（S403）、ヘッドホン2から存在情報の返送をもらう（S404）。そして、通信認証装置1はミュージックプレーヤー3に対してヘッドホン2の存在を通知し（S405）、ミュージックプレーヤー3はヘッドホン2との接続を完了する（S406）。従って、ミュージックプレーヤー3で再生する音楽をヘッドホン2によって受信して利用することができる。

【0029】図5は、第1のデバイス2が小型送受話装置であり、第2のデバイス3が携帯電話であって、両者の接続認証を通信認証装置1で行うものである。ここで携帯電話3は、通信網55を経由して他の携帯電話、又はその他の通信機器と接続して音声その他のデータの送受信を行うものである。小型送受話装置2が携帯電話3に接続要求を出すと（S501）、携帯電話3は通信認証装置1に対して接続してよいデバイスかどうか確認問い合わせをする（S502）。通信認証装置1は小型送受話装置2の存在をチェックし（S503）、小型送受話装置2から存在情報の返送をもらう（S504）。通信認証装置1は携帯電話3に小型送受話装置2の存在を通知し（S505）、携帯電話3は小型送受話装置2との接続を完了する（S506）。従って、携帯電話3で送受信するデータを小型送受話装置2によって送受信して利用することができる。

【0030】図6から図10は、本発明の他の実施例による通信認証方法を示すブロック図である。図6は第1のデバイス2が音楽データ記録装置であり、第2のデバイス3がデジタルラジオであって、両者の接続認証を通信認証装置1で行うものである。音楽データ記録装置2がデジタルラジオ3に接続要求を出し（S601）、デジタルラジオ3は通信認証装置1に対して接続してよいデバイスかどうか確認問い合わせをする（S602）。通信認証装置1は音楽データ記録装置2の装置アドレスをチェックし（S603）、音楽データ記録装置2から装置アドレスを返送させる（S604）。通信認証装置1は返送された装置アドレスが、通信認証装置1内部の記憶手段7に記憶されているアドレスであるか照合する（S605）。通信認証装置1はデジタルラジオ3に音楽データ記録装置2へのデータ送信を許可し（S606）、デジタルラジオ3は放送局54から受信した音楽データを音楽データ記録装置2へ送信する（S607）。

【0031】図7は第1のデバイス2が携帯端末装置で

あり、第2のデバイス3がファイルストレージ装置であって、両者の接続認証を通信認証装置1で行うものである。携帯端末装置2がファイルストレージ装置3にファイル要求を出し（S701）、ファイルストレージ装置3は通信認証装置1に対して接続してよいデバイスかどうか確認問い合わせをする（S702）。通信認証装置1は携帯端末装置2の装置アドレスをチェックし（S703）、携帯端末装置2から装置アドレスを返送させる（S704）。通信認証装置1は返送された装置アドレスが、通信認証装置内部の記憶手段7に記憶されているアドレスであるか照合する（S705）。通信認証装置1はファイルストレージ装置3に携帯端末装置2へファイルオープンを許可し（S706）、ファイルストレージ装置3は携帯端末装置2へファイルオープンして送信する（S707）。

【0032】図8は第1のデバイス2が電話装置であり、第2のデバイス3が公衆網用ゲートウェイであって、両者の接続認証を通信認証装置1で行うものである。電話装置2が公衆網用ゲートウェイ3に接続要求を出し（S801）、公衆網用ゲートウェイ3は通信認証装置1に対して接続してよいデバイスかどうか確認問い合わせをする（S802）。通信認証装置1は電話装置2の装置アドレスをチェックし（S803）、電話装置2から装置アドレスを返送させる（S804）。通信認証装置1は返送された装置アドレスが、通信認証装置内部の記憶手段7に記憶されているアドレスであるか照合する（S805）。通信認証装置1は公衆網用ゲートウェイ3に電話装置2への接続を許可し（S806）、公衆網用ゲートウェイ3は公衆網55からの通信を中継して電話装置2へ転送する（S807）。

【0033】図9は第1のデバイス2が電子メール/Web端末装置であり、第2のデバイス3がインターネットアクセス装置であって、両者の接続認証を通信認証装置1で行うものである。電子メール/Web端末装置2がインターネットアクセス装置3に接続要求を出し（S901）、インターネットアクセス装置3は通信認証装置1に対して接続してよいデバイスかどうか確認問い合わせをする（S902）。通信認証装置1は電子メール/Web端末装置2の装置アドレスをチェックし（S903）、電子メール/Web端末装置2から装置アドレスを返送させる（S904）。通信認証装置1は返送された装置アドレスが、通信認証装置内部の記憶手段7に記憶されているアドレスであるか照合する（S905）。通信認証装置1はインターネットアクセス装置3に電子メール/Web端末装置2との接続許可を出し（S906）、インターネット57からの電子メールやWebデータを、インターネットアクセス装置3を介して電子メール/Web端末装置2へ転送する（S907）。

【0034】図10は第1のデバイス2が電話装置であ

り、第2のデバイス3が音声データ記録装置であって、両者の接続認証を通信認証装置1で行うものである。電話装置2が音声データ記録装置3に通話録音要求を出し（S101）、音声データ記録装置3は通信認証装置1に対して接続してよいデバイスかどうか確認問い合わせをする（S102）。通信認証装置1は電話装置2の装置アドレスをチェックし（S103）、電話装置2から装置アドレスを返送させる（S104）。通信認証装置1は返送された装置アドレスが、通信認証装置内部の記憶手段7に記憶されているアドレスであるか照合する（S105）。通信認証装置1は音声データ記録装置3に電話装置2からの音声データの録音許可を出し（S106）、公衆網55から公衆網用ゲートウェイ56を経由して電話装置2で交信されている音声データを音声データ記録装置3で録音する（S107）。

【0035】図11は、本発明の他の実施例による通信認証方法を示すブロック図である。本実施例は、第1のデバイス2が携帯端末装置であり、第2のデバイス3がインターネットアクセス装置であって、両者の接続認証を通信認証装置1で行うものである。通信認証装置1がインターネットアクセス装置3に情報要求を出し（S111）、インターネットアクセス装置3は通信認証装置1に対してどのような携帯端末装置2に接続可能か問い合わせをする（S112）。通信認証装置1は利用可能な携帯端末装置2を検索し（S113）、携帯端末装置2を使用者が操作する（S114）ことにより、携帯端末装置2から通信認証装置1に装置アドレスが返送される（S115）。通信認証装置1は返送された装置アドレスをインターネットアクセス装置3に通知する（S116）。インターネットアクセス装置3は通知された装置アドレスを持つ携帯端末装置2に対してインターネット57からの情報を送信する（S117）。

【0036】図12は、本発明の他の実施例による通信認証方法を示すブロック図である。本実施例は、第1のデバイス2が携帯端末装置であり、第2のデバイス3がインターネットアクセス装置であって、両者の接続認証を通信認証装置1で行うものである。通信認証装置1がインターネットアクセス装置3に情報要求を出し（S111）、インターネットアクセス装置3は通信認証装置1に対してどのような携帯端末装置2に接続可能か問い合わせをする（S112）。通信認証装置1は利用可能な携帯端末装置2を検索し（S113）、携帯端末装置2を使用者が操作する（S114）ことにより、携帯端末装置2から通信認証装置1に装置アドレスが返送される（S115）。通信認証装置1は返送された装置アドレスが、通信認証装置内部の記憶手段7に記憶されているアドレスであるか照合する（S126）。通信認証装置1は返送された装置アドレスをインターネットアクセス装置3に通知する（S127）。インターネットアクセス装置3は通知された装置アドレスを持つ携帯端末装



置2に対してインターネット57からの情報を送信する(S128)。

【0037】図13は、本発明の他の実施例による通信認証方法を示すブロック図である。本実施例は、第1のデバイス2が携帯電話等の表示機能を持った端末装置であり、第2のデバイス3がレジスター装置であって、両者の接続認証を通信認証装置1で行うものである。レジスター装置3から通信認証装置1に決裁情報を要求し(S131)、通信認証装置1は決裁要求のあったレジスター装置アドレスが、通信認証装置内部の記憶手段7に記憶されているアドレスであるか照合する(S132)。通信認証装置1は、決裁可能である情報(表示を行う表示装置2を特定する情報を含む)をレジスター装置3に通知する(S133)。レジスター装置3は合計金額を、特定された携帯電話2に通知し(S134)、携帯電話2の利用者は合計金額の確認をレジスター装置3に送り(S135)、インターネット57を介して金融機関等で決裁される。ここで、S131の決裁情報にこれから精算すべき顧客の携帯電話2の装置アドレスを含めて送信し、通信認証装置1では、既に登録済みの顧客であるかの判断により決裁可能かどうかの判断することにより更にセキュリティを強化できる。

【0038】図14は、本発明の他の実施例による通信認証方法を示すブロック図である。本実施例は、第1のデバイス2は1台であり、第2のデバイス3が、n台まで複数である構成の通信認証方法である。第2のデバイス3から第1のデバイス2に接続要求を出し(S141)、第1のデバイス2が第2のデバイス3へ接続してよいかどうかを、第1のデバイス2から通信認証装置1へ問い合わせ(S142)、通信認証装置1が第2のデバイス3の存在をチェックし(S143)、第2のデバイス3から装置アドレスを返送する(S144)。通信認証装置1は返送された装置アドレスが、通信認証装置内部の記憶手段7に記憶されているアドレスであるか照合する(S145)。通信認証装置1は第1のデバイス2に対して、第2のデバイス3との接続許可を送り(S146)、第1のデバイス2と第2のデバイス3とのデータ通信が開始される(S147)。以上の通信認証を複数台順次認証していく。また、通信認証装置1にあらかじめ通信形態を登録しておくことによって、ブルートゥース通信に規定されているマスターとスレーブの装置関係の決定もできる。

【0039】本実施例による通信認証方法は、通信認証装置と無線通信で接続されていて、互いに第1のデバイスと1:1の関係で無線接続されている第2のデバイスから第n(nは自然数)のデバイスにおいて、第1のデバイスから第2のデバイスに接続要求を出すステップと、第1のデバイスが第2のデバイスへ接続してよいかどうかを、第1のデバイスから通信認証装置へ問い合わせるステップと、通信認証装置が第2のデバイスの装置

アドレスを確認するステップと、第2のデバイスから装置アドレスを返送するステップと、返送された装置アドレスが通信認証装置内部の記憶手段に記憶されているアドレスであるか照合するステップと、通信認証装置が第1のデバイスに対して、第2のデバイスとの接続許可を送信するステップと、第1のデバイスと第2のデバイスの接続を完了するステップとを有している。そして、第1のデバイスと第2のデバイスの接続が完了するまでのステップを、第nのデバイスまで順次繰り返し行うものである。本実施例によれば、無線通信エリア内にある1台の通信認証装置を用いて第1のデバイスと1:1の関係でn台まで順次認証していくことができる。また、本実施例によると、会議室に会議参加メンバーの所有するブルートゥースを搭載したモバイルコンピュータが持ち込まれ、会議参加メンバーに資料を配付していく場合などにおいても、強固にセキュリティを保持できる。

【0040】また本実施例による通信認証方法は、通信認証装置と無線通信で接続されていて、互いに第1のデバイスと1:1の関係で無線接続されている第2のデバイスから第n(nは自然数)のデバイスにおいて、第1のデバイスから第2のデバイスに接続要求を出すステップと、第1のデバイスが第2のデバイスへ接続してよいかどうかを、第1のデバイスから通信認証装置へ問い合わせるステップと、通信認証装置が第2のデバイスの装置アドレスを確認するステップと、第2のデバイスから装置アドレスを返送するステップと、返送された装置アドレスが通信認証装置内部の記憶手段に記憶されているアドレスであるか照合するステップと、通信認証装置が第1のデバイスに対して、第2のデバイスとの接続許可を送信するステップと、第1のデバイスと第2のデバイスの接続を完了するステップとを有する。そして、通信認証装置にあらかじめ設定された通信形態に従って、第1のデバイスと第2のデバイスの接続が完了するまでのステップを、第nのデバイスまで順次繰り返し行う。本実施例によれば、無線通信エリア内にある1台の通信認証装置を用いて、あらかじめ通信認証装置に設定登録した通信形態に従って、第1のデバイスと1:1の関係でn台まで順次認証していくことができる。また、本実施例によると、会議室などであらかじめ設定しておいた通信形態に基づいて、会議参加メンバーの所有するブルートゥースを搭載したモバイルコンピュータを認証していくので、より強固にセキュリティを保持することができる。なお、本実施例では、通信認証を複数台順次認証するとしたが、同時に複数台の認証を行う構成であってもよい。

【0041】図15は、本発明の他の実施例による通信認証方法を示すブロック図である。本実施例は、第1のデバイス2は1台であり、第2のデバイス3が、n台まで複数であるが、それぞれのデバイスがブルートゥース通信のマスター装置であり、またそれぞれにスレーブ装

置が複数台接続されている場合の通信認証方法である。第2のデバイス(3から第nのデバイス3n)まで順次接続認証をし(S151)、同時にそれぞれに接続されたスレーブを、通信認証装置1にあらかじめ設定した構成に従ってネットワークから切り離す(S152)。次に、通信認証装置1は第1のデバイス2をマスター装置に選定し(S153)、第1のデバイス2と第2のデバイス(スレーブ装置)3とのデータ通信が開始される。そして第n番目の第2のデバイス(スレーブ装置)3nまでデータ通信を行う。また、通信認証装置1をマスター装置として、第1番目から第n番目の第2のデバイス3をスレーブ装置として通信認証したあとで、スレーブ装置とした第2のデバイス3中の1台を新たなマスター装置として構成してもよい。また、本実施例における通信認証方法は、将来的にウェアブル化されたパーソナルコンピュータをマスター装置として身に付け、その周辺に各種モバイル装置をスレーブ装置として接続した状態の人間が複数名で1つの会議室に集結した場合に、セキュリティを確保しながら、あらかじめ設定した通信形態に容易に移行できる。

【0042】本実施例による通信認証方法は、通信認証装置が一台設置されていて、第1のデバイスと1:1の関係で無線接続されている第2のデバイスから第n(nは自然数)のデバイスからなるネットワークが複数個、同一無線通信エリア内に集結した通信形態を前提とする。そして、集結した各々のネットワークの内、代表の1つのデバイスを、あらかじめ通信認証装置に登録されているアドレス情報に基づいて、集結したネットワークの数と同じか、それ以下の数だけ、順次認証していくステップと、代表の1つのデバイス(認証完了したデバイス)を複数個集めて、あらかじめ通信認証装置に設定しているネットワークを形成するステップと、複数個のデバイスの内、マスターとなる1台を選択認証するステップと、マスターのデバイスと1:1の関係で、その他の代表のデバイスと通信を開始するステップとを有する。本実施例によれば、無線通信エリア内に1台の通信認証装置を設置し、そのエリア内に1:nで構成された複数個のネットワークが集結した場合、集結した個々のネットワーク中の1台を、あらかじめ通信認証装置に登録されている装置アドレス情報に基づいて認証し、その認証したデバイスの内の1台をマスターとして、新しく構成されたネットワークの中心装置として通信を開始することができるので、ブルートゥース端末装置等の無秩序な通信を防止できる。

【0043】図16は、本発明の他の実施例による通信認証方法を示すブロック図である。本実施例は、第1のデバイス2は1台であり、第2のデバイス3が、n台まで複数であるが、それぞれのデバイスがブルートゥース通信のマスター装置であり、またそれぞれのマスター装置に通信認証装置1台とスレーブ装置が複数台接続され

ている場合の通信認証方法である。本実施例は、複数の通信認証装置間で先に近距離無線通信によって接続し、あらかじめ通信認証装置1に登録されている優先順位情報に基づいて最上位通信認証装置を決定し(S161)、各々の通信認証装置から、最上位通信認証装置に対して各々の通信認証装置に接続されているデバイスの内、代表の1台のデバイスのアドレス情報を通知し(S162)、その他のデバイスはネットワークから切り離す(S163)。最上位通信認証装置は、登録されているアドレス情報と装置構成に基づいてデバイスを順次認証していく(S164)、認証を完了したデバイスの内の1台をマスター装置と指定して(S165)、その他のデバイスをスレーブ装置として通信を開始する(S166)。また、本実施例では、n台全てのデバイスを認証する形態で説明したが、通信認証装置1に設定されているn台よりも少ない台数を認証し、元マスター装置であったデバイスにスレーブ装置として接続されていたデバイスを最終的な通信形態で通信可能にするものであってもよい。また、本実施例における通信認証方法は、将来的にウェアブル化されたパーソナルコンピュータをマスター装置として身に付け、その周辺に通信認証装置と各種モバイル装置をスレーブ装置として接続した状態の人間が複数名で1つの会議室に集結した場合に、セキュリティを確保しながら、あらかじめ設定した通信形態に容易に移行できる。

【0044】本実施例による通信認証方法は、通信認証装置と無線通信で接続されていて、互いに第1のデバイスと1:1の関係で無線接続されている第2のデバイスから第n(nは自然数)のデバイスからなるネットワークが複数個、同一無線通信エリア内に集結した通信形態を前提とする。そして、集結した各々のネットワークの内、代表の1つの通信認証装置を、あらかじめ通信認証装置に登録されている優先順位情報に基づいて最上位通信認証装置として決定するステップと、各々の通信認証装置から、最上位通信認証装置に対して、集結した各々のネットワーク中の代表のデバイスのアドレス情報を通知するステップと、集結した各々のネットワーク中の内、代表の1つのデバイスを、最上位の通信認証装置に登録されているアドレス情報に基づいて、順次認証していくステップと、代表の1つのデバイス(認証完了したデバイス)を複数個を集めて、あらかじめ通信認証装置に設定しているネットワークを形成するステップと、複数個のデバイスの内、マスターとなる1台を選択認証するステップと、マスターのデバイスと、1:1の関係で、その他の代表のデバイスと通信を開始するステップとを有する。本実施例によれば、デバイスn台と通信認証装置1台の組み合わせで同一の無線通信エリアに集結した場合に、集結した複数台の通信認証装置の内の1台が、あらかじめ通信認証装置に登録されている優先順位情報に基づいて最上位通信認証装置として決定され、他

の通信認証装置と接続されていたデバイスを装置アドレス情報に基づいて順次認証し、その認証したデバイスの内の1台をマスターとして、新しく構成されたネットワークの中心装置として通信を開始することができるので、ブルートゥース端末装置等の無秩序な通信を防止できる。なお、図4から図16までのそれぞれの通信認証装置1における認証手段として、使用者の指紋、角膜、遺伝子等の人体固有の生体情報を検出して認証を行う機能を付加することにより、機密保持をより一層強固なものにできる。

【0045】次に、通信認証装置1のパスワードによる通信認証について、通信認証装置1へのパスワード登録方法とデバイスを認証する際のパスワード解除方法を、図17から図22を用いて説明する。図17から図22は、本発明の一実施例によるパスワードによる通信認証方法を示すフロー図である。

【0046】図17に記載の通信認証方法は、まず使用者がパスワード入力で通信許可をもらう際に、通信認証装置から質問させる形式を、あらかじめ設定しておく

(S171)、複数の無線デバイスを、パスワードを用いて登録する時、使用者の氏名、生年月日、電話番号、電子メールアドレス、免許証番号など複数の実際の個人データをパスワードとして入力し(S172)、入力したパスワードを通信認証装置1のメモリ部7に記憶する(S173)。次に、複数の無線デバイスを通信エリア内で通信可能にする際は、あらかじめ使用者が設定した質問形式で質問される内容の回答を、デバイスから通信認証装置1にデータを入力して送信し(S174)、入力によって回答したデータと通信認証装置1のメモリ部7に記憶された使用者の個人データを比較し(S175)、比較した結果が一致した場合には通信を許可し、複数の無線デバイスを使用可能とする(S176)。S175で不一致の場合には、再度回答を入力して送信し(S174)、入力したデータと通信認証装置1のメモリ部7に記憶された使用者の個人データを比較する(S175)。なお、セキュリティの面から、この不一致の場合の回答回数を所定回数に限ることが好ましい。認証の際の質問形式の設定にあたっては、例えば複数の内の1つのパスワードを質問、複数の内の2つのパスワードを質問、又は複数の内の所定数のパスワードを質問させ、登録されているパスワードの中から質問形式と一致するパスワードが入力された場合に通信を許可する。また、質問形式はデバイス毎に変更し、デバイス特有のパスワードを選択させる場合であってもよい。また通信接続する2つのデバイスによって、複数のパスワードの内の特有のパスワードを選択する場合であってもよい。また、通信の接続時間帯や、エリアによって複数のパスワードの内の特有のパスワードを選択する場合であってもよい。また、パスワードに関して、本実施例では、実際の個人データをパスワードとして入力する場合で説明し

たが、使用者が設定したユニークな識別番号又は識別記号であってもよい。ここで説明した質問形式の設定、及びパスワードに関しては、本実施例に限らず下記で説明する実施例においても適用できる。

【0047】本実施例による通信認証方法は、複数の無線デバイスを扱う通信システムにおいて、複数の無線デバイスをパスワードで登録し、しかる後に複数の無線デバイスを使用する段階では、パスワード入力で通信許可とする通信認証装置の通信認証方法である。本実施例による通信認証方法は、使用者がパスワード入力で通信許可をもらう際に、通信認証装置から質問させる形式を、あらかじめ設定しておくステップと、複数の無線デバイスを、パスワードを用いて登録する時、使用者の氏名、生年月日、電話番号、電子メールアドレス、免許証番号など複数の実際の個人データをパスワードとして入力するステップと、入力したパスワードを通信認証装置のメモリ部に記憶するステップと、複数の無線デバイスを通信エリア内で通信可能にする際、あらかじめ使用者が設定した質問形式で質問される内容の回答を、通信認証装置にデータ入力するステップと、入力したデータと通信認証装置のメモリ部に記憶された使用者の個人データを比較するステップと、比較した結果が一致した場合には通信を許可し、複数の無線デバイスを使用可能とするステップとを有する。本実施例によれば、通信エリア内で使用するデバイスの装置アドレスの他に、使用者自身に由縁のある氏名、生年月日、電話番号、電子メールアドレス、免許証番号等の情報をパスワードとして登録するので、忘却する危険性が少なく、パスワードを書き留める必要がない。また、使用認証時のパスワード入力は、あらかじめ使用者が定義しておいた質問形式に対して、複数個の答えを手動で入力するので使用者本人であれば正解を入力できるので、第三者による通信認証装置の不正使用の防止策となる。また、本実施例では、パスワードは、手動入力で説明したが、音声認識による入力方法であってもよい。

【0048】図18に記載の通信認証方法は、まず使用者がパスワード入力で通信許可をもらう際に、通信認証装置から質問させる形式を、あらかじめ設定しておく(S171)、複数の無線デバイスを、パスワードを用いて登録する時、使用者の氏名、生年月日、電話番号、電子メールアドレス、免許証番号など複数の実際の個人データをパスワードとして入力し(S172)、入力したパスワードを通信認証装置のメモリ部に記憶する(S173)。次に、複数の無線デバイスを通信エリア内で通信可能にする際は、あらかじめ使用者が設定した質問形式で質問される内容の回答が、デバイスから自動的に通信認証装置1に対して送信され(S184)、複数の無線デバイスを使用可能とする(S176)。

【0049】本実施例による通信認証方法は、複数の無線デバイスを特定の無線通信エリアで取り扱う通信シス

テムにおいて、複数の無線デバイスをパスワードで登録し、しかる後に複数の無線デバイスを使用する段階では、パスワード入力で通信許可とする通信認証装置の通信認証方法である。本実施例による通信認証方法は、使用者が、パスワード入力で通信許可をもらう際に、通信認証装置から質問させる形式を、通信認証装置にあらかじめ設定しておくステップと、複数の無線デバイスを、パスワードを用いて登録する時、使用者の氏名、生年月日、電話番号、電子メールアドレス、免許証番号など複数の実際

10 数の実際の個人データをパスワードとして入力するステップと、入力したパスワードを通信認証装置のメモリ部に記憶するステップと、使用者が、通信認証装置を特定の無線通信エリアに持ち込んだ時は、自動的にあらかじめ使用者が設定した質問形式で質問される内容の回答を、通信認証装置にデータ入力されるステップと、入力したデータと通信認証装置のメモリ部に記憶された使用者の個人データを比較するステップと、比較した結果が一致した場合には通信を許可し、複数の無線デバイスを使用可能とするステップとを有する。本実施例によれば、通信エリア内で使用するデバイスの装置アドレスの他に、使用者自身に由縁のある氏名、生年月日、電話番号、電子メールアドレス、免許証番号等の情報をパスワードとして登録するので、忘却する危険性が少なく、パスワードを書き留める必要がない。また、通信認証装置を特定の無線通信エリアに持ち込んだ時は、自動でパスワード入力されるので、通信認証装置の存在を意識することなく快適にセキュリティを保持できる。

【0050】図19に記載の通信認証方法は、まず使用者がパスワード入力で通信許可をもらう際に、通信認証装置から質問させる形式を、あらかじめ設定しておく（S171）、複数の無線デバイスを、パスワードを用いて登録する時、使用者の氏名、生年月日、電話番号、電子メールアドレス、免許証番号など複数の実際の個人データをパスワードとして入力し（S172）、入力したパスワードを通信認証装置のメモリ部に記憶する（S173）。次に、使用者が特定の無線通信エリアに進入した時、鍵を挿入、又は使用されたことを検出し（S191）、あらかじめ使用者が設定した質問形式で質問される内容の回答を、デバイスから通信認証装置1にデータを入力して送信し（S174）、入力によって回答したデータと通信認証装置1のメモリ部7に記憶された使用者の個人データを比較し（S175）、比較した結果が一致した場合には通信を許可し、複数の無線デバイスを使用可能とする（S176）。また、本実施例では、固定された場所に設置してある通信認証装置で認証を行う場合の他、自動車等の移動するエリア内に通信認証装置が設置されている場合の認証であってもよい。また、通信認証装置を持ち歩いている場合であってもよい。また、本実施例では、S174での質問の回答を使用者が入力したが、自動入力であれば更に素早く認証が行え

る。

【0051】本実施例による通信認証方法は、使用者が特定の無線通信エリアに進入した時の、特定無線通信エリアの認識と確定には、通信認証装置に鍵を挿入するか、あるいは鍵が特定場所で使用されたことを検出した電気信号による位置検出手段を利用するものである。本実施例によれば、家屋のドアロックシステムとの連動や、鍵による集中管理システムに利用することができる。また、通信認証装置が設置されている場合でも、通信認証装置を持ち歩いている場合でも、鍵の使用という別の目的のための動作の2次的な作用によって、その通信エリアが特定されて通信認証が開始されるので、通信認証装置の存在を意識することなく強固にセキュリティを保持できる。また、特定の無線通信エリアは、自動車の室内等の移動する空間であっても、鍵の使用によって確実に通信認証ができる。

【0052】図20に記載の通信認証方法は、使用者がパスワード入力で通信許可をもらう際に、通信認証装置から質問させる形式を、あらかじめ設定しておく（S171）、複数の無線デバイスを、パスワードを用いて登録する時、使用者の氏名、生年月日、電話番号、電子メールアドレス、免許証番号など複数の実際の個人データをパスワードとして入力し（S172）、入力したパスワードを通信認証装置のメモリ部に記憶する（S173）。次に、使用者が特定の無線通信エリアに進入した時、鍵の挿入、又は使用されたことを検出後、通信認証装置をスタンバイモードから起動状態にし（S201）、あらかじめ使用者が設定した質問形式で質問される内容の回答を、デバイスから通信認証装置1にデータを入力して送信し（S174）、入力によって回答したデータと通信認証装置1のメモリ部7に記憶された使用者の個人データを比較し（S175）、比較した結果が一致した場合には通信を許可し、複数の無線デバイスを使用可能とする（S176）。また、本実施例では、固定された場所に設置してある通信認証装置で認証を行う場合の他、自動車等の移動するエリア内に通信認証装置が設置されている場合の認証であってもよい。また、通信認証装置を持ち歩いている場合であってもよい。また、本実施例では、S174での質問の回答を使用者が入力したが、自動入力であれば更に素早く認証が行える。

【0053】本実施例による通信認証方法は、使用者が特定の無線通信エリアに進入した時の、特定無線通信エリアの認識と確定には、通信認証装置に鍵を挿入するか、あるいは鍵が特定空間で使用されたことを検出した電気信号による位置検出手段を利用し、位置検出手段で検出した位置情報に基づいて、通信認証装置をスタンバイ状態から起動状態にするものである。本実施例によれば、通信認証装置が設置されている場合でも、通信認証装置を持ち歩いている場合でも、鍵の使用という別の目

的のための動作の２次的な作用によって、その通信エリアが特定されて通信認証装置が起動状態になるので、通信認証装置の存在を意識することなく強固にセキュリティを保持できる。また、通信認証装置の消費電力を減少させることができる。

【００５４】図２１に記載の通信認証方法は、まず使用者がパスワード入力で通信許可をもらう際に、通信認証装置から質問させる形式を、あらかじめ設定しておく

（Ｓ１７１）、複数の無線デバイスを、パスワードを用いて登録する時、使用者の氏名、生年月日、電話番号、電子メールアドレス、免許証番号など複数の実際の個人データをパスワードとして入力し（Ｓ１７２）、入力したパスワードを通信認証装置のメモリ部に記憶する（Ｓ１７３）。次に、使用者が通信認証装置を特定の無線通信エリアに持ち込んだ時は、通信認証装置に搭載されたＧＰＳやＰＨＳ等の位置検出手段を利用して位置を確定し（Ｓ２１１）、あらかじめ使用者が設定した質問形式で質問される内容の回答を、デバイスから通信認証装置１にデータを入力して送信し（Ｓ１７４）、入力によって回答したデータと通信認証装置１のメモリ部７に記憶された使用者の個人データを比較し（Ｓ１７５）、比較した結果が一致した場合には通信を許可し、複数の無線デバイスを使用可能とする（Ｓ１７６）。また、本実施例では、Ｓ１７４での質問の回答を使用者が入力したが、自動入力であれば更に素早く認証が行える。また、特定の無線通信エリアを複数登録しておけば、複数の場所での認証も可能になる。

【００５５】本実施例による通信認証方法は、使用者が通信認証装置を特定の無線通信エリアに持ち込んだ時の、特定無線通信エリアの認識と確定には、通信認証装置に搭載されたＧＰＳやＰＨＳ等の位置検出手段を利用するものである。本実施例によれば、使用者がＧＰＳやＰＨＳによる位置検出手段を搭載した通信認証装置を持ち歩き、その通信認証装置を使用者があらかじめ位置設定した場所（無線通信エリア）に持ち込んだ時のみ、パスワードによる通信認証が開始されるので、強固にセキュリティを保持できる。

【００５６】図２２に記載の通信認証方法は、まず使用者がパスワード入力で通信許可をもらう際に、通信認証装置から質問させる形式を、あらかじめ設定しておく

（Ｓ１７１）、複数の無線デバイスを、パスワードを用いて登録する時、使用者の氏名、生年月日、電話番号、電子メールアドレス、免許証番号など複数の実際の個人データをパスワードとして入力し（Ｓ１７２）、入力したパスワードを通信認証装置のメモリ部に記憶する（Ｓ１７３）。次に、使用者が通信認証装置を特定の無線通信エリアに持ち込んだ時は、通信認証装置に搭載されたＧＰＳやＰＨＳ等の位置検出手段を利用して位置を確定し、通信認証装置をスタンバイモードから起動状態にし（Ｓ２２１）、あらかじめ使用者が設定した質問形式で

質問される内容の回答を、デバイスから通信認証装置１にデータを入力して送信し（Ｓ１７４）、入力によって回答したデータと通信認証装置１のメモリ部７に記憶された使用者の個人データを比較し（Ｓ１７５）、比較した結果が一致した場合には通信を許可し、複数の無線デバイスを可能とする（Ｓ１７６）。また、本実施例では、Ｓ１７４での質問の回答を使用者が入力したが、自動入力であれば更に素早く認証が行える。また、特定の無線通信エリアを複数登録しておけば、複数の場所での認証も可能になる。

【００５７】本実施例による通信認証方法は、使用者が通信認証装置を特定の無線通信エリアに持ち込んだ時の、特定無線通信エリアの認識と確定には、通信認証装置に搭載されたＧＰＳやＰＨＳ等の位置検出手段を利用して、位置検出手段で検出した位置情報に基づいて、通信認証装置をスタンバイ状態から起動状態にするものである。本実施例によれば、使用者がＧＰＳやＰＨＳによる位置検出手段を搭載した通信認証装置を持ち歩き、その通信認証装置を使用者があらかじめ位置設定した場所（無線通信エリア）に持ち込んだ時のみ、通信認証装置が起動状態になるので、より強固にセキュリティを保持できる。

【００５８】上記実施例においてＳ１７４では、複数の無線デバイスを通信エリア内で通信可能にする際、あらかじめ使用者が設定したパスワードがランダムに質問されるものであってもよい。また、Ｓ１７６では、通信認証装置のタイマー手段であらかじめ設定した時間経過後に、通信を開始するものであってもよい。この場合には、通信エリア内のデバイスを認証した後、通信認証装置に設定されている時間経過後に通信を開始するので、会議室などでメンバーが集まり、会議スタート時点からのデータ交信となり、機密情報が事前に配布されることがない。また、Ｓ１７６では、通信開始した後、通信認証装置のタイマー手段であらかじめ設定した時間経過後に通信を強制終了させるものであってもよい。通信開始した後、通信認証装置のタイマー手段であらかじめ設定した時間経過後に、通信を強制終了させるものである。通信エリア内のデバイスを認証し通信を開始した後、通信認証装置に設定されている時間経過後に通信を終了するので、管理者（使用者）が通信エリアから離れる場合や、会議室などで会議終了後しばらくしてのデータ交信終了をしたい場合などに利用でき、機密情報が管理者（使用者）の意に反して配布されることがない。また、上記実施例による通信認証方法において、複数の無線デバイスを通信認証装置にパスワードで登録する時、使用者の氏名、生年月日、電話番号、電子メールアドレス、免許証番号など複数の実際の個人データをパスワードとして入力し、入力したパスワードを通信認証装置のメモリ部に所定の暗号化アルゴリズムに基づいて、暗号化して記憶するものであってもよい。この場合には、通信認



証装置にデバイスや通信形態を登録するとき用いたパスワードが暗号化保存されているので、第三者による故意のパスワード盗み出しに対処できる。また、上記実施例による通信認証方法において、通信認証装置からランダムな組み合わせや順序でパスワードを出すことで、前回の通信認証のパスワード入力時に盗み見られた場合でも、強固にセキュリティを保持できる。また、本実施例による通信認証方法の全てか、あるいは単独、あるいは複数の組み合わせを備えたプロトコル制御プログラムを記録媒体に格納し、または通信網を介してダウンロードすることもできる。そしてこのプログラムをブルートゥースによる通信が可能なモバイルコンピュータやパームOSコンピュータにインストールまたはダウンロードすることにより、通信認証装置として使用することができる。なお、本実施例での「データ通信」とは、正式な使用者が意図した実データの交信であって、接続前のブルートゥース方式のモバイル端末や家電装置間の接続要求等の装置が勝手に行うプロトコルは含まない。

【0059】図23は、本発明の他の実施例による通信認証方法を示すブロック図である。本実施例は、第1のデバイス2がハンドセット等の通信機能を持った端末装置であり、第2のデバイス3がモバイルルーターであって、両者の接続認証を通信認証装置1で行うものである。ハンドセット2からモバイルルーター3に接続要求(S231)をすると、モバイルルーター3から通信認証装置1に接続確認の問い合わせが発行される(S232)。通信認証装置1はハンドセット2が使用者本人の所有物であり、かつ通信認証装置1も使用者本人の所有物である検証を指紋認証により実施し(S233)、認証結果をモバイルルーター3に通知する(S234)。ハンドセット2が使用者本人の所有物であり、かつ通信認証装置1も使用者本人の所有物である認証結果はモバイルルーターからインターネットを介して認証サーバ58で再度検証され接続許可の通知が来る(S235)。モバイルルーター3は接続許可通知(S235)に基づいて、ハンドセット2との通信を開始する(S236)。そして、ハンドセット2は電話網55を利用して通話(S237)できるようになる。なお、上記実施例では、通信認証装置1において、ハンドセット2が使用者本人の所有物であり、かつ通信認証装置1も使用者本人の所有物であることの検証を指紋認証により実施したが、指紋認証をしないで通信認証装置1内にあらかじめ格納されている個人情報のみの検証でも可能である。

【0060】図24は、本発明の他の実施例による通信認証方法を示すブロック図である。本実施例は、第1のデバイス2がメール端末やWeb端末等の通信機能を持った端末装置であり、第2のデバイス3がモバイルルーターであって、両者の接続認証を通信認証装置1で行うものである。メール端末/Web端末2からモバイルルーター3に接続要求(S241)をすると、モバイルル

ーター3から通信認証装置1に接続確認の問い合わせが発行される(S242)。通信認証装置1はメール端末/Web端末2が使用者本人の所有物であり、かつ通信認証装置1も使用者本人の所有物である検証を指紋認証により実施し(S243)、認証結果をモバイルルーター3に通知する(S244)。メール端末/Web端末2が使用者本人の所有物であり、かつ通信認証装置1も使用者本人の所有物である認証結果はモバイルルーターからインターネットを介して認証サーバ58で再度検証され接続許可の通知が来る(S245)。モバイルルーター3は接続許可通知(S245)に基づいて、メール端末2との通信を開始する(S246)。そして、メール端末/Web端末2はインターネット57に接続可能となる。なお、上記実施例では、通信認証装置1において、メール端末/Web端末2が使用者本人の所有物であり、かつ通信認証装置1も使用者本人の所有物であることの検証を指紋認証により実施したが、指紋認証をしないで通信認証装置1内にあらかじめ格納されている個人情報のみの検証でも可能である。

【0061】図25は、本発明の他の実施例による通信認証方法を示すブロック図である。本実施例は、第1のデバイス2がリモコン装置であり、第2のデバイス3がモバイルルーターであり、第3のデバイス59が表示装置であって、3者の接続認証を通信認証装置1で行うものである。リモコン2からモバイルルーター3に番組選択指示(S251)をすると、モバイルルーター3から通信認証装置1に使用者の番組視聴契約内容等の接続確認問い合わせが発行される(S252)。通信認証装置1はリモコン操作者の番組選択指示内容と、通信認証装置1内にあらかじめ格納されている番組視聴契約情報や個人情報の照合、および通信認証装置1がリモコン操作者本人の所有物である検証を指紋認証により実施し(S253)、認証結果をモバイルルーター3に通知する(S254)。リモコン2が操作者本人の所有物であり、かつ通信認証装置1も使用者本人の所有物である認証結果と選択された番組は、モバイルルーターからインターネットを介して認証サーバ58で再度検証され接続許可の通知が来る(S255)。モバイルルーター3は接続許可通知(S255)に基づいて、放送局54から供給される(S256)番組を表示装置59に送信し(S257)、番組が表示装置59に表示される。なお、上記実施例では、通信認証装置1において、リモコン2が操作者本人の所有物であり、かつ通信認証装置1も使用者本人の所有物であることの検証を指紋認証により実施したが、指紋認証をしないで通信認証装置1内にあらかじめ格納されている個人情報のみの検証でも可能である。

【0062】図26は、本発明の他の実施例による通信認証方法を示すブロック図である。本実施例は、第1のデバイス2がクレジットカードであり、第2のデバイス

3 がレジスターであって、クレジットカード 2 で支払いをする際に、通信回線を使用して決済するための通信認証を通信認証装置 1 で行うものである。クレジットカードの情報を読み取りレジスター 3 へ通知すると (S 2 6 1)、レジスター 3 から通信認証装置 1 へ、クレジットカード番号等のカードから読み取ったデータを送信する (S 2 6 2)。通信認証装置 1 はクレジットカードが正当かつ有効な使用者本人の所有物であり、かつ通信認証装置 1 も使用者本人の所有物である検証を指紋認証により実施し (S 2 6 3)、認証結果をレジスター 3 に通知する (S 2 6 4)。クレジットカードが正当かつ有効な使用者本人の所有物であり、かつ通信認証装置 1 も使用者本人の所有物である認証結果はレジスターから通信回線を介してクレジットカードセンター 6 0 に送信され (S 2 6 5)、ここで初めてカード番号の照会を含めた詳細な検証された使用許可 (決済許可) の通知が来る (S 2 6 5)。レジスター 3 は使用許可 (決済許可) の通知 (S 2 4 5) に基づいて、クレジットカードによる決済を行う。なお、上記実施例では、クレジットカード 2 は通常の磁気データ式のカードを想定しているが、IC カードや無線通信可能なカード等でクレジットカードの機能を備えたものであってもよい。また、上記実施例において、クレジットカード 2 のクレジットカードセンター 6 0 で再度行う際に、初めてカード番号の照会を含めた詳細な検証がされるので、販売店のレジスターにはカードの詳細情報は残存せず、極めて強固な機密保持が可能となる。なお、上記実施例におけるクレジットカードセンター 6 0 は、クレジット以外のカードセンターであってもよい。

【0063】図 27 は、本発明の他の実施例による通信認証方法を示すブロック図である。本実施例は、第 2 のデバイス 3 が入場門や玄関扉等のゲートあり、ゲート 3 を開ける際に、通信回線を使用してゲートを開けるための認証を通信認証装置 1 で行うものである。ゲートを開ける希望者は、希望者個人が所有する通信認証装置 1 が正当かつ有効な使用者本人の所有物であることを、内部に予め格納されている個人情報を含めて指紋認証により検証を実施し (S 2 7 1)、通信認証装置 1 からゲート 3 に、通信認証装置 1 の内部に予め格納されている個人情報や入門予約情報を通知する (S 2 7 2)。ゲート 3 は通信認証装置から受け取ったデータを通信回線を介して認証サーバ 5 8 に送信し (S 2 7 3)、認証サーバ 5 8 はゲートを開くためのデータとして有効であるか検証する。認証サーバ 5 8 からゲート 3 に、ゲートオープン可能の通知が送られ (S 2 7 4)、ゲート 3 はゲートを開ける (S 2 7 5)。また、上記実施例において、認証サーバ 5 8 で検証を行うにあたっては、利用者個人の指紋情報を扱うものではなく、通信認証装置 1 の内部に予め格納されている個人情報や入門予約情報の検証を行うものである。よって、指紋情報等の極めて機密性の高い

生体情報が外部に漏洩することはない。

#### 【0064】

【発明の効果】上記説明から明らかなように、本発明によれば、無線通信が可能なエリア内にある 2 台以上の通信装置とは別に存在する通信認証装置によって、エリア内にある 2 台以上の通信装置について通信を行うか否かを認証して通信を行うことができる。また、通信を行うか否かを認証方法として、個人の生体情報 (指紋、角膜、遺伝子等) を利用することにより、より強固な機密保持が可能となる。また、通信機器間の通信機密保持のための暗号化手段と組み合わせて利用することにより、更に強固な機密保持が可能となる。

#### 【図面の簡単な説明】

【図 1】 本発明の一実施例による通信認証装置の機能ブロック図

【図 2】 本発明の一実施例による通信認証装置の機能ブロック図

【図 3】 本発明の一実施例による通信認証装置の機能ブロック図

20 【図 4】 本発明の一実施例による通信認証方法を説明するための構成図

【図 5】 本発明の一実施例による通信認証方法を説明するための構成図

【図 6】 本発明の一実施例による通信認証方法を説明するための構成図

【図 7】 本発明の一実施例による通信認証方法を説明するための構成図

【図 8】 本発明の一実施例による通信認証方法を説明するための構成図

30 【図 9】 本発明の一実施例による通信認証方法を説明するための構成図

【図 10】 本発明の一実施例による通信認証方法を説明するための構成図

【図 11】 本発明の一実施例による通信認証方法を説明するための構成図

【図 12】 本発明の一実施例による通信認証方法を説明するための構成図

【図 13】 本発明の一実施例による通信認証方法を説明するための構成図

40 【図 14】 本発明の一実施例による通信認証方法を説明するための構成図

【図 15】 本発明の一実施例による通信認証方法を説明するための構成図

【図 16】 本発明の一実施例による通信認証方法を説明するための構成図

【図 17】 本発明の一実施例によるパスワードによる通信認証方法を説明するフロー図

【図 18】 本発明の一実施例によるパスワードによる通信認証方法を説明するフロー図

50 【図 19】 本発明の一実施例によるパスワードによる



通信認証方法を説明するフロー図

【図20】 本発明の一実施例によるパスワードによる通信認証方法を説明するフロー図

【図21】 本発明の一実施例によるパスワードによる通信認証方法を説明するフロー図

【図22】 本発明の一実施例によるパスワードによる通信認証方法を説明するフロー図

【図23】 本発明の一実施例による通信認証方法を説明するための構成図

【図24】 本発明の一実施例による通信認証方法を説明するための構成図

【図25】 本発明の一実施例による通信認証方法を説明するための構成図

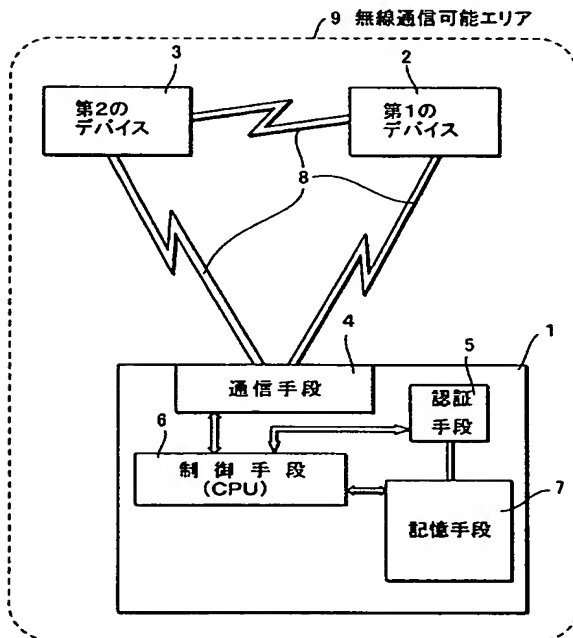
【図26】 本発明の一実施例による通信認証方法を説明するための構成図

【図27】 本発明の一実施例による通信認証方法を説明するための構成図

【符号の説明】

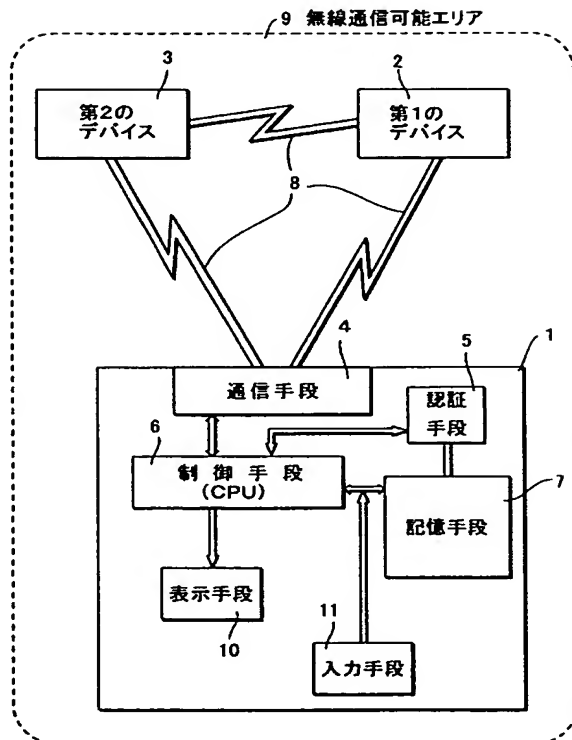
- 1 通信認証装置
- 2 第1のデバイス
- 3 第2のデバイス
- 4 通信手段
- 5 認証手段

【図1】

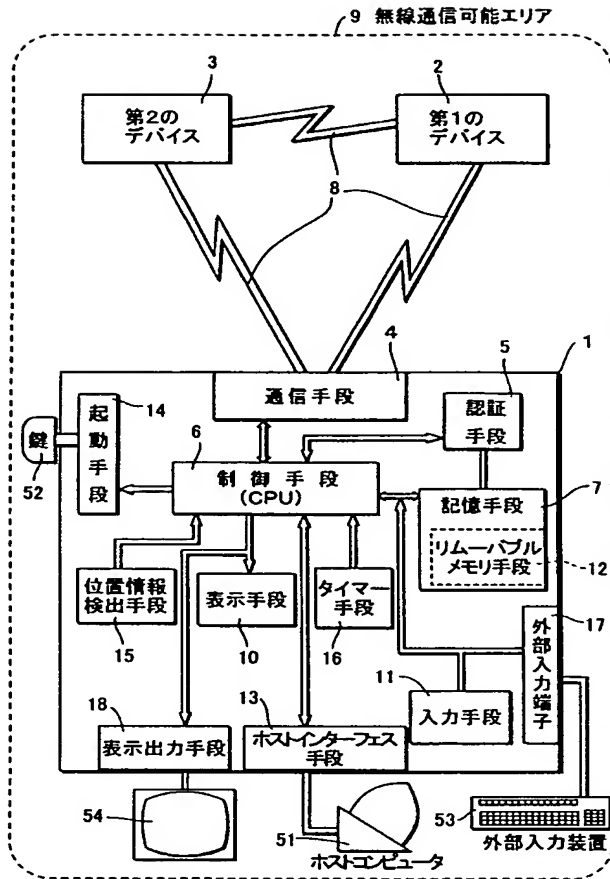


- 6 制御手段
- 7 記憶手段
- 8 通信回線
- 9 無線通信可能エリア
- 10 表示手段
- 11 入力手段
- 12 リムーバブルメモリ手段
- 13 ホストインターフェイス手段
- 14 起動手段
- 15 位置情報検出手段
- 16 タイマー手段
- 17 外部入力端子
- 18 表示出力手段
- 51 ホストコンピュータ
- 52 鍵
- 53 外部入力装置
- 54 放送局
- 55 公衆網
- 56 公衆網用ゲートウェイ
- 57 インターネット
- 58 認証サーバ
- 59 第3のデバイス
- 60 クレジットカードセンター

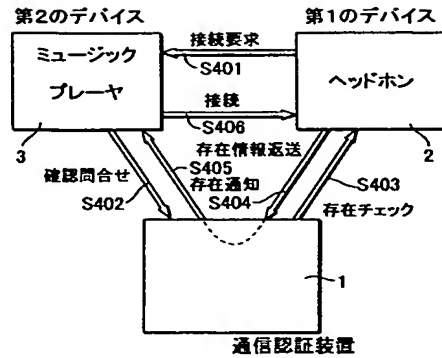
【図2】



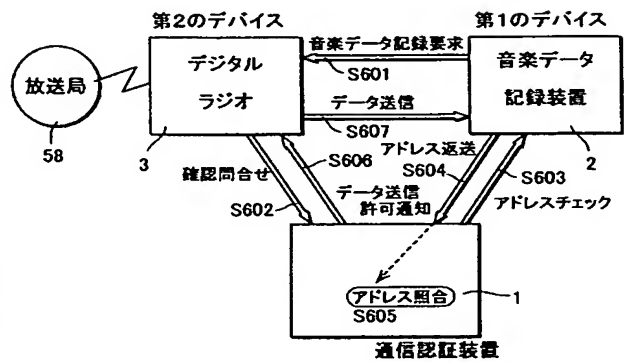
【図3】



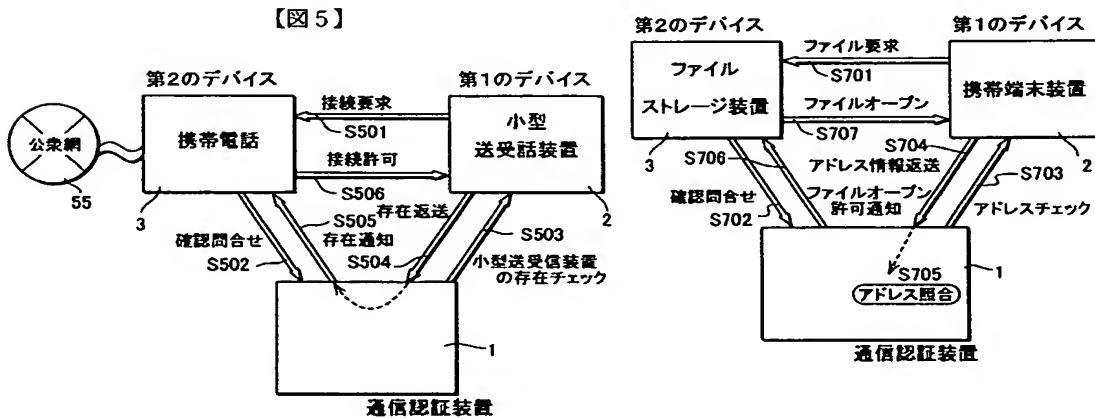
【図4】



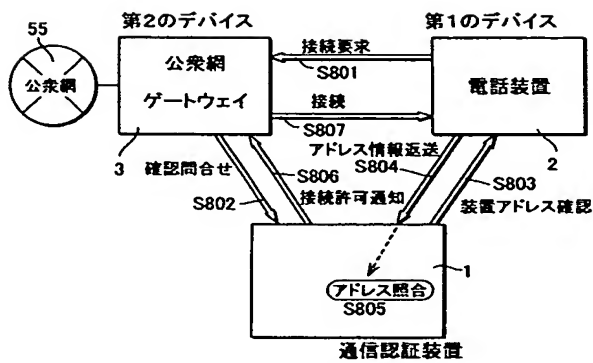
【図6】



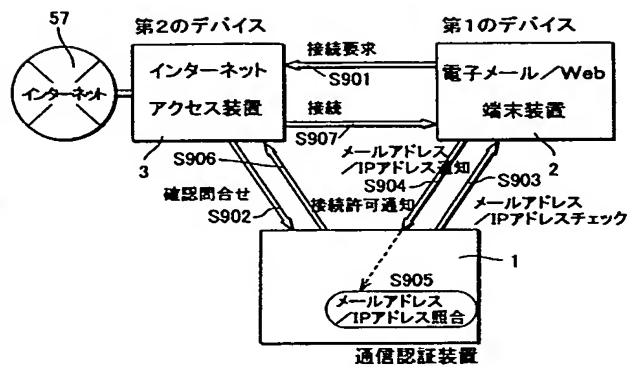
【図7】



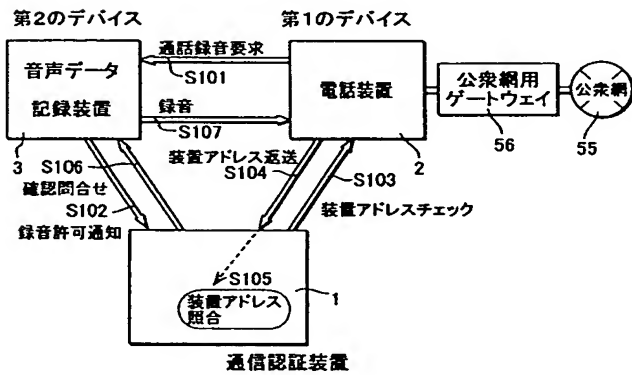
【図8】



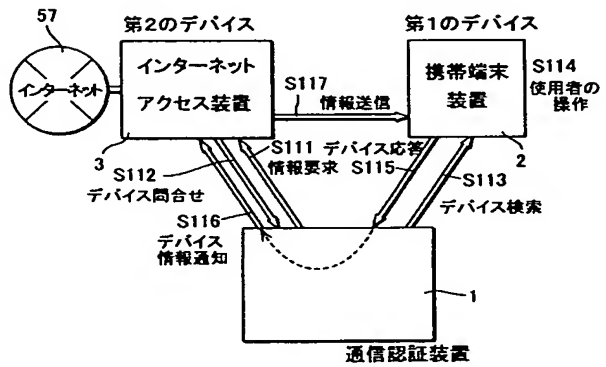
【図9】



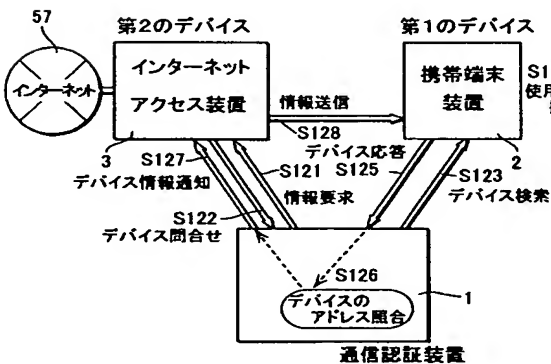
【図10】



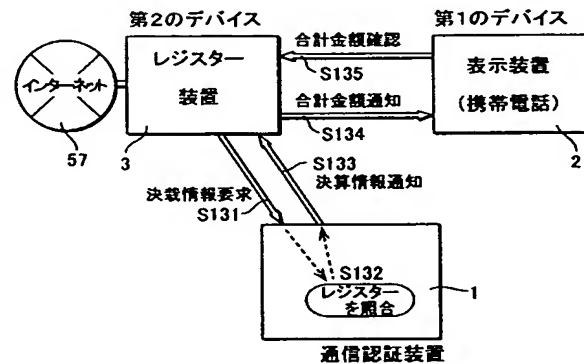
【図11】



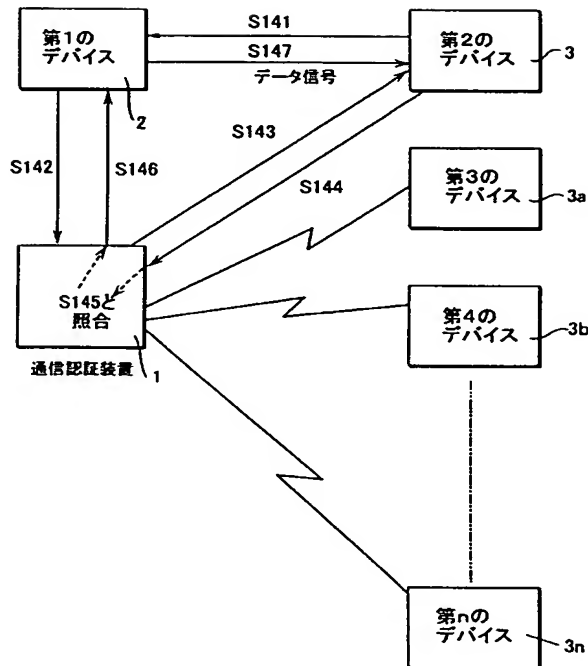
【図12】



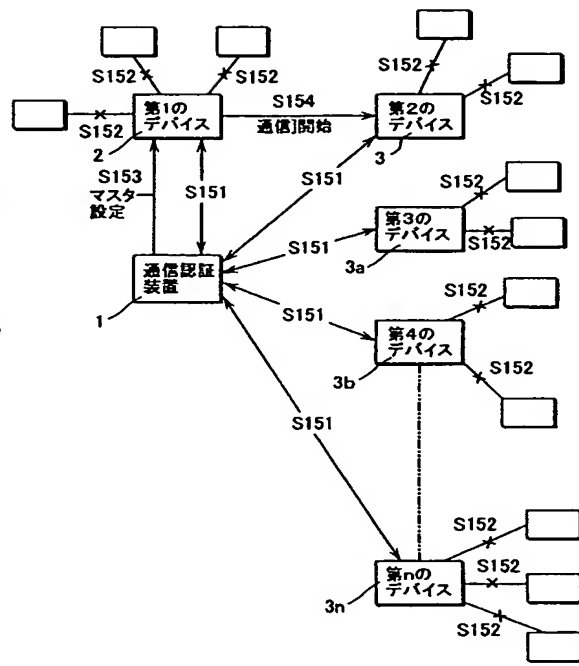
【図13】



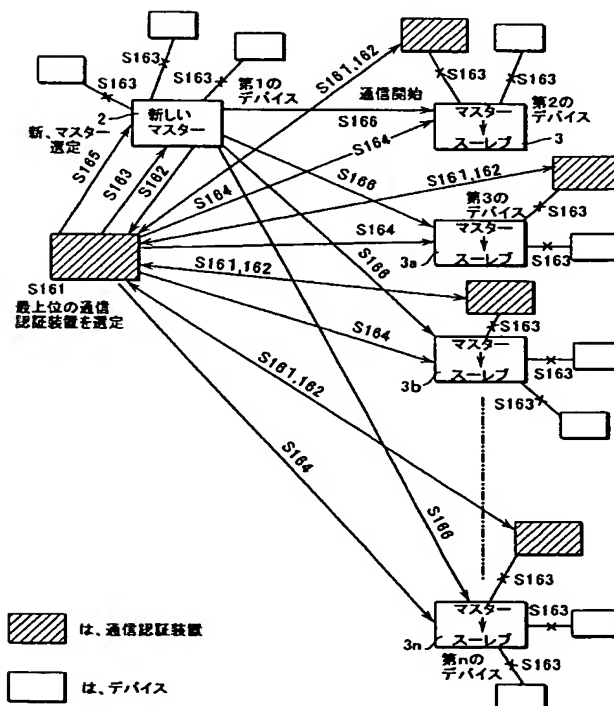
【図14】



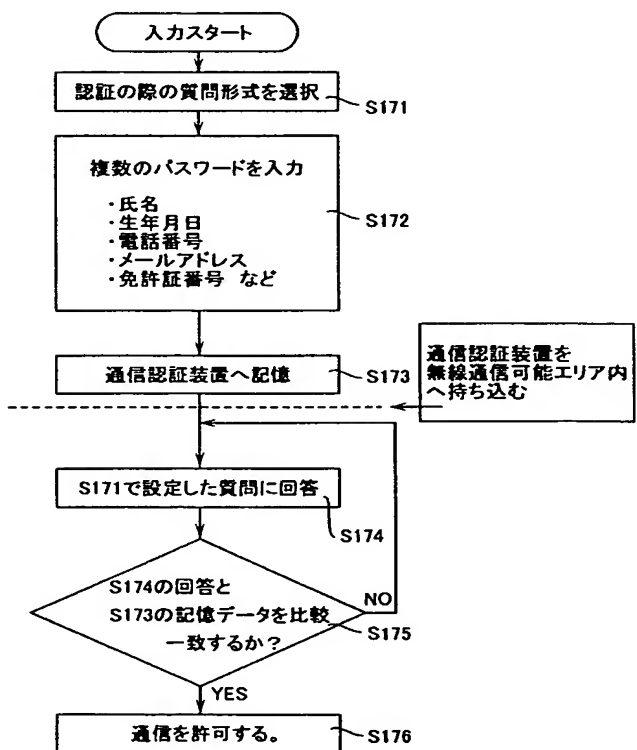
【図15】



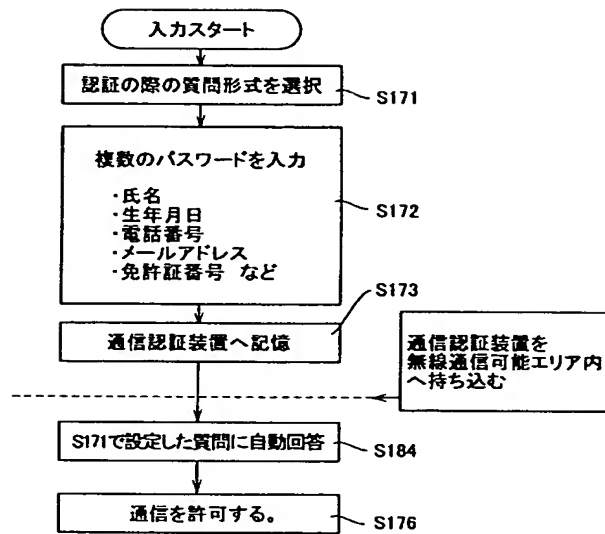
【図16】



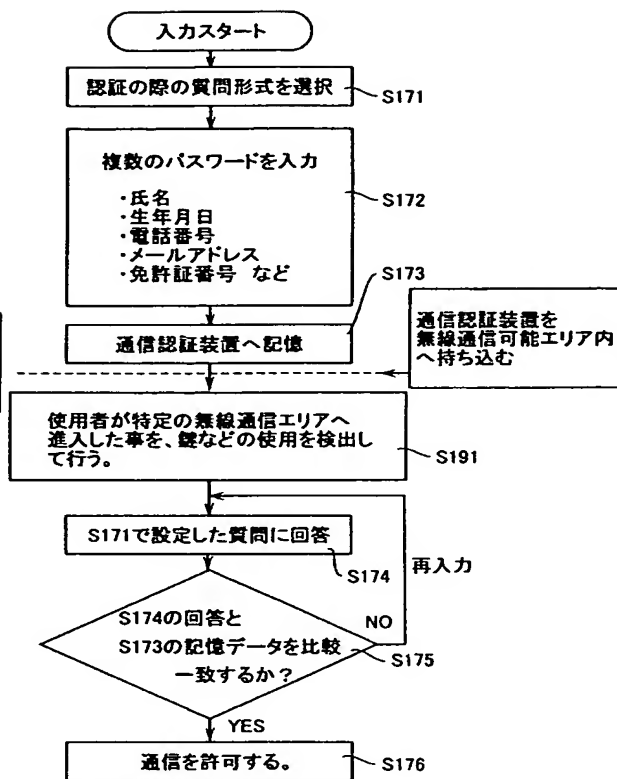
【図17】



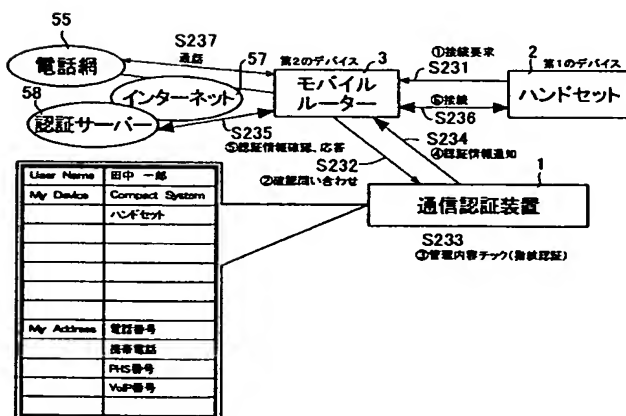
【図18】



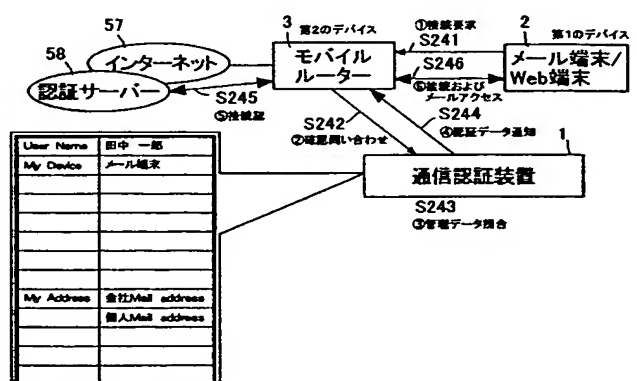
【図19】



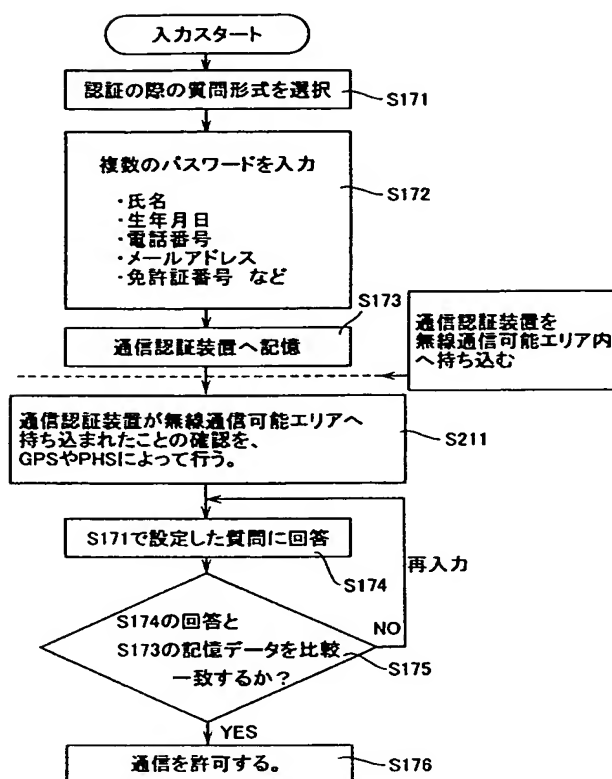
【図23】



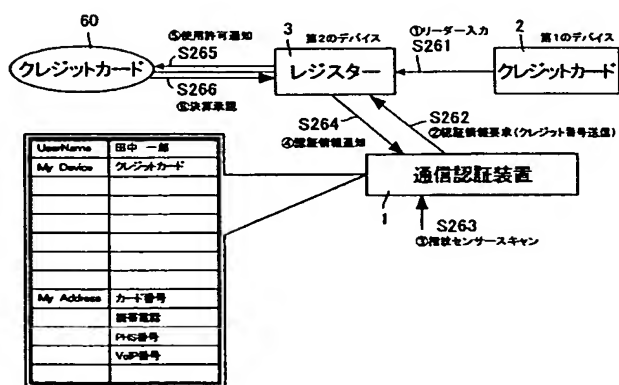
【図24】



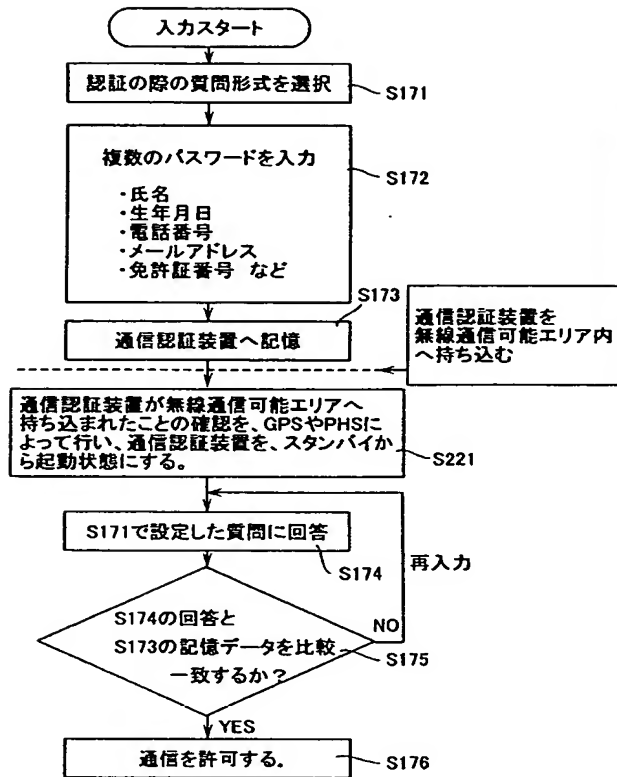
【图 2 1】



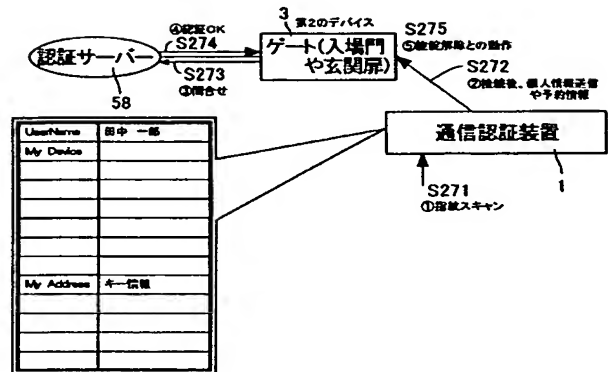
【图 2 6】



【図22】



【図27】



フロントページの続き

(72)発明者 松田 俊介  
東京都品川区南大井6-17-17 FINE  
ビル 株式会社イーウィズユー内

(72)発明者 三室 悟  
東京都品川区南大井6-17-17 FINE  
ビル 株式会社イーウィズユー内

F ターム(参考) 5B085 AA08 AE02 AE03 AE15 AE23  
BC01 BE01 BE04 BG02  
5J104 AA07 KA02 KA06 KA16 MA01  
NA05 PA01 PA07  
5K033 AA08 CB01 DA19 DB12 EC01  
EC03  
5K067 AA30 BB01 BB21 DD04 DD17  
EE02 EE10 EE16 HH36 KK13  
KK15